03-09-05　　　　　2827
　　　　　　　　BFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:　　　　　　　　:
　　　　　　　　　　　　　　　　　　　:
　　　　Kevin Kwong-Tai CHUNG　　　　: Art Unit:　2827
　　　　　　　　　　　　　　　　　　　:
Appl. Serial No. 09/737,306　　　　　　: Examiner:　Mark S. Tremblay
　　　　　　　　　　　　　　　　　　　:
Filed:　　　December 15,2000　　　　　: Confirmation No. 1695
　　　　　　　　　　　　　　　　　　　:
For:　　　ELECTRONIC VOTING APPARATUS,
　　　　　SYSTEM AND METHOD　　　　:

TRANSMITTAL LETTER FOR THE
DECLARATION OF KEVIN KWONG-TAI CHUNG

Filed herewith is the Declaration of Kevin Kwong-Tai Chung Under 37 C.F.R. §1.132 which is submitted in support of the patentability of the captioned Patent Application.

Specifically, Declarant sets forth that there is a long-felt need for an electronic voting machine, system and method that provides the capability for a full audit of the votes cast electronically in an election, and that the voting machine, system and method claimed in the captioned Application can satisfy that long-felt need. Several articles are presented as Exhibits in support of the fact that there is a long-felt need for such voting machine, system and method. In addition, aspects of Applicant's claimed invention provide for voter verification of his votes cast on an electronic voting machine and/or system that can later be audited, and provide a corresponding method.

Declarant further sets forth that the reasons presented in the Response filed with the

1

BEST AVAILABLE COPY

Request for Continued Examination are in fact correct and support patentability.

Therefore Applicant's claims as presently pending are not obvious and are patentable, and so should be allowed.

Applicant respectfully requests that this Declaration and the facts set forth therein be fully considered and that the pending claims be allowed and passed to issuance.

No fee is due inconsequence of this submission. Should any fee be due, please charge such fee to Deposit Account 04-1406.

The Examiner is requested to telephone the undersigned attorney if there is any question or if prosecution of this Application could be furthered by telephone.

> Respectfully submitted,
> Dann, Dorfman, Herrell & Skillman, P.C.
> Attorneys for Applicant(s)
>
> By: _Clement A. Berard_
> Clement A. Berard
> PTO Registration No. 29,613

March 8, 2005

Dann, Dorfman, Herrell and Skillman, P.C.   Telephone: 215-563-4100
1601 Market Street, Suite 2400   Facsimile: 215-563-4044
Philadelphia, PA 19103

In re the Application of: :
:
        Kevin Kwong-Tai CHUNG   : Art Unit: 2827
:
Appl. Serial No. 09/737,306   : Examiner: Mark S. Tremblay
:
Filed: December 15, 2000   : Confirmation No. 1695
:
For: ELECTRONIC VOTING APPARATUS,:
         SYSTEM AND METHOD   :

Certificate of Mailing Under 37 C.F.R. §1.8(a)

I hereby certify that this Correspondence, along with any paper referred to as being attached or enclosed, is being deposited on the Certificate Date below with the United States Postal Service with sufficient postage as first-class mail in an envelope addressed to COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, VA 22313-1450.

March 8, 2005
Date of Certificate

Jacqueline D. Bailey
By: JACQUELINE D. BAILEY

DECLARATION OF KEVIN KWONG-TAI CHUNG UNDER 37 C.F.R. §1.132

I, KEVIN KWONG-TAI CHUNG, HEREBY DECLARE AND SAY:

1.   I am an inventor named in the captioned U.S. Patent Application No. 09/737,306 filed December 15, 2000 and entitled "ELECTRONIC VOTING APPARATUS, SYSTEM AND METHOD."

2.   I am President of Amerasia International Technology, Inc., located in Princeton Junction, New Jersey, to which my captioned U.S. Patent Application is assigned.

3.   I am President of Avante International Technology, Inc., located in Princeton Junction, New Jersey, which is marketing VOTE-TRAKKER™ voting machines including the invention claimed in my captioned Patent Application as well as other voting apparatus. VOTE-TRAKKER™ voting machines marketed by Avante include an embodiment of the invention claimed in my captioned Patent Application and have been certified as being in compliance with U.S. Federal (NASED) voting standards and with the voting standards of more than fifteen (15) states, including California, Ohio and New Jersey.

4.   I was awarded the Bachelor of Arts degree in Physics by Rutgers University in 1974

1

and the Doctor of Philosophy degree in Materials Science by Rutgers University in 1982.

5.   I have been engaged in the development of voting apparatus and systems including electronic voting machines and other devices, systems and methods relating to voting for over four years. I am the author of over five technical papers and articles relating to the subject of voting and have given testimony before the United States Congress and the Election Assistance Commission (EAC) relating to voting, voting apparatus and voting methods. I am a named inventor in about ten Patent Applications relating to the subject of voting apparatus and methods, and in about forty other Patents and Patent Applications.

6.   The invention claimed in my captioned U.S. Patent Application relates to voting apparatus and method wherein a voting session identifier for each voting session is stored with a representation of the vote cast in that voting session both in a memory of the voting apparatus and in a tangible medium (e.g., a voter-verified paper record) separate from the voting apparatus. The voting session identifier is unique for each voting session and is unrelated to the identity of the voter. As a result, votes cast as recorded by the voting apparatus may be audited by comparison to the votes recorded in the tangible medium on a vote-by-vote basis, e.g., by comparing the votes recorded in the memory for a particular voting session with the votes recorded in the tangible medium (e.g., a voter-verified paper record) for that voting session.

7.   A problem with conventional direct recording electronic (DRE) voting machines is that there is no way to audit the accuracy and correctness of the votes cast as recorded in the memory thereof. Recounting simply recalls and recounts the same votes cast as stored in the memory of the voting machine, even in plural memories thereof, and so the recount will always match the initial readout. There is no "audit trail" or other way to verify that the votes cast as stored in one or more memories of a conventional DRE voting machine accurately and correctly reflect the voter's intended votes. Errors in recording the votes cast, whether arising from a systemic or a random event, or even "errors" introduced intentionally to affect the election outcome, cannot be detected. This has led to widespread suspicion and distrust of conventional DRE voting machines. Thus, there is a long felt need for a DRE voting machine and method that overcomes the shortcomings of conventional DRE voting machines.

8.   Evidence of this long-felt need is found, for example, in many published articles. A 1993 paper by Peter G. Neumann titled "Security Criteria for Electronic Voting" (a copy of which is appended hereto as Exhibit A), which was published before the filing date of the captioned Patent Application, states in the paragraph bridging from page 5 to 6 that:

        "The requirement for voter confidentiality and the requirement for nonsubvertible and sufficiently complete end-to-end monitoring are conceptually contradictory. It is essentially impossible to achieve both at the

same time without resorting to complicated mechanisms, which themselves
may introduce new potential vulnerabilities and opportunities for more
sophisticated subversions." (underline added).

My claimed voting machine, system and method solves the problem that Dr.
Neumann deems "conceptually contradictory" and "essentially impossible."

9.   Further evidence of this long felt and unsatisfied need is found in Dr. Rebecca
      Mercuri's 2001 article titled "Rebecca Mercuri's Statement on Electronic Voting" (a
      copy of which is appended hereto as Exhibit B), which was published after the present
      Application was filed:

      "Fully electronic systems do not provide any way that the voter can truly
      verify that the ballot cast corresponds to that being recorded, transmitted, or
      tabulated....
      Electronic ballot systems without individual print-outs for examination by the
      voters, do not provide an independent audit trail...."

      My claimed voting machine, system and method provides an individual print out and
      also provides an audit trail auditable on a vote-by-vote basis.

10.   Further evidence of this long felt and unsatisfied need is found in Dr. Rebecca
      Mercuri's 2003 article titled "A Better Ballot Box" (a copy of which is appended
      hereto as Exhibit C), which was published after the present Application was filed,
      wherein Dr. Mercuri states:

      "These problems result from an underlying fundamental conflict in the
      construction of electronic voting (e-voting) systems: the simultaneous need
      for privacy and auditability, which is the ability, when necessary, to recount
      the votes cast.... In other words, the privacy constraint directly conflicts with
      the ability to audit the ballot data." (page 46, right column)

and

      "The Mercuri Method allows voters to check that their votes will be recorded
      accurately by requiring that electronic voting machines be modified to
      generate paper ballots. Such a system does not exist, but could be created by
      machine manufacturers." (page 47, Figure caption; underline added)

      My claimed voting machine, system and method not only provides what Dr. Mercuri
      now advocates, but it further provides an audit trail auditable on a vote-by-vote basis,
      thereby overcoming the "direct conflict" described by Dr. Mercuri.

11.   The controversy over whether DRE voting machines should or should not be utilized
      continues. For example:
      a.   David Dill et al "Frequently Asked Questions about DRE Voting Systems"
            which was found at http://www.verifiedvoting.org/drefaq.asp (a copy
            of which is appended hereto as Exhibit D). Dill et al specifically notes
            in Section 3.1 the Avante Vote-Trakker™ voting system which
            embodies my claimed arrangement and its having been certified in
            California, and which provides a voter-verified paper trail.

b.   Open Voting Consortium (OVC), "Frequently Asked Questions (FAQ),"
which was found at http://www.openvotingconsortium.org/faq.html (a
copy of which is appended hereto as Exhibit E). This article describes
an "open voting" system that includes a printed paper ballot to provide
a voter-verified paper trail, as does my claimed voting machine, system
and method.

c.   Verified Voting Foundation, "E-Voting Misconceptions" which was found at
http://www.verifiedvoting.org/article.asp?id=2609 (a copy of which is
appended hereto as Exhibit F). This article reports that Federal
legislation that would mandate a voter-verified paper record, as is
provided by my claimed voting machine, system and method, is under
consideration.

d.   Alan Dechert's "Statement at Utah State Capital, July, 2003," which was
found at http://www.openvotingconsortium.org/ad/alan-ut-7-13.html
(a copy of which is appended hereto as Exhibit G). Dechert states that
California has mandated a paper record of voting, as is provided by my
claimed voting machine, system and method.

e.   M. Shamos, "Paper v. Electronic Voting Records – An Assessment," which
was found at
http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm#_edn1 (a
copy of which is appended hereto as Exhibit H). This article which
argues that a paper ballot is not the solution to concern surrounding the
use of DRE voting machines is criticized in the article cited in sub-
paragraph f. below.

f.   "OVC Response to Paper v. Electronic Voting Records – An Assessment, by
Michael Shamos" which was found at
http://gnosis.python-hosting.com/voting-project/July.2004/0240.html
(a copy of which is appended hereto as Exhibit I). This article
criticizes the Shamos article cited in sub-paragraph e. above and argues
for printed paper trails.

12.   There is a long felt need for an electronic voting machine that overcomes the problem
arising from the lack of any auditability in a conventional electronic voting machine.
My voting machine, system and method as claimed in the captioned Application
addresses and provides a novel and unobvious solution that provides the ability to
perform an audit of electronic voting while still protecting the anonymity of the voter.
Moreover, my claimed arrangement can not only provide confidence in the
cumulative vote totals, but can also permit an audit to be performed on a vote-by-vote
basis, if desired, while still maintaining the voter's privacy.

13.   The State of California banned electronic voting machines that do not produce a
voter-verified paper trail that can authenticate that the vote was recorded accurately,
according to an article by K. Zetter dated April 30, 2004 entitled "California Bans E-
Voting" which was found at http://www.wirednews.com/news/evote/0,2645,63298-

2,00.html?tw=wn_story_page_next1 (a copy of which is appended hereto as Exhibit J). This article mentions the Avante Vote-Trakker™ voting machine that includes an embodiment of my invention that provides a voter-verified paper record and that has been certified by Federal and state authorities.

14.   A simple paper receipt does not satisfy the long-felt need because it lacks "transparency" as reported by the Associated Press on February 3, 2005, in an article entitled "Prototype E-Vote Printer Fails to Satisfy" (a copy of which is appended hereto as Exhibit K). The tangible receipt as recited in the claims of my captioned Application does provide transparency, thereby satisfying the long-felt need, because a unique and randomized voting session identifier is associated with each voting session and is recorded with the vote in the voting machine and is stored in the tangible receipt.

15.   There is a long felt need for an electronic voting machine that overcomes the problem arising from the lack of any auditability in an electronic voting machine. My voting machine, system and method as claimed in the captioned Application addresses and provides a novel and unobvious solution that provides the ability to perform an audit of electronic voting while still protecting the anonymity of the voter, thereby satisfying that long felt need. Moreover, my claimed arrangement can not only provide confidence in the cumulative vote totals, but can also permit an audit to be performed on a vote-by-vote basis, if desired, while still maintaining the voter's privacy.

16.   An advantage of my claimed invention is that the voting information stored in the tangible medium cannot be changed by the voting apparatus, either through an intentional or an accidental action, after a voting session ends, and so is completely independent of the voting machine and available to provide independent authentication of the vote.

17.   In the captioned Application, the Examiner has applied several references relating to smart card security and credit card transactions in rejecting the claims of the captioned Application. These references provide for complete openness and traceability wherein any transaction can be reconstructed from one of many complete and partial redundant records thereof. The requirements of such systems are significantly different from the requirement of a voting system and method for transparency on one hand, and anonymity of the voter on the other hand. These references teach away from what my invention is directed to and so cannot anticipate or render my invention obvious. The arguments for patentability set forth on pages 26-39 of the Request for Continued Examination and Response to Final Office Action filed on or about November 22, 2004, are incorporated herein by reference as if set forth herein in their entirety.

18.   To my knowledge, my invention is the first to satisfy the long felt need for auditability

5

in an electronic voting machine, system and method. My invention is the first to provide for a voter-verified record and vote-by-vote auditability. My invention is first to provide for a voter-verified record and vote-by-vote auditability to be embodied in a practical apparatus.

19.   I find no description or suggestion in the applied references of a voting session identifier that is unique for each voting session and is unrelated to the identity of the voter, and that is associated with the record of votes cast as stored in a memory of a voting machine and on a tangible medium (e.g., voter-verifiable paper receipt) with which a vote-by-vote audit may be conducted, as claimed in my captioned U.S. Patent Application.

All statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code (18 U.S.C. § 1001) and may jeopardize the validity of the patent application or any patent issuing thereon.

Declarant: KEVIN KWONG-TAI CHUNG

Signature: _____   Date: 3/7/05

Security Criteria for Electronic Voting

Peter G. Neumann
Computer Science Laboratory
SRI International, Menlo Park CA 94025
1-650-859-2375 Neumann@csl.sri.com

[Copyright 1993, Peter G. Neumann. This paper was presented at the 16th National Computer Security Conference Baltimore, Maryland, September 20-23, 1993.]

Abstract. Some basic criteria for confidentiality, integrity, availability, reliability, and assurance are considered for computer systems involved in electronic voting. An assessment of the realizability of those criteria leads to the conclusion that, operationally, many of the criteria are inherently unsatisfiable with any meaningful assurance.

BACKGROUND

The election processes of voter registration, vote casting, vote counting, and ballot generation are becoming increasingly automated [Sal93]. Numerous cases of allegedly accidental errors have been reported, along with suspicions of fraud [Dug88,Neu90]. However, the borderline between accident and fraud is murky. Serious security vulnerabilities are commonplace in most voting systems, providing widespread opportunities for computer-system misuse --- particularly by insiders [NeuPar89,Mer93]. Indeed, incentives for bribery, collusion, and fraud are likely to be enhanced by the financial stakes involved in winning or losing an election.

At present there is no generally accepted standard set of criteria that voting systems are required to satisfy. This paper proposes a generic set of criteria similar in concept to existing security criteria such as the U.S. TCSEC (the Orange Book, TNI, TDI, etc.), the European ITSEC, the Canadian CTCPEC, and the draft U.S. Federal Criteria. We observe that essentially all existing voting systems would fail to satisfy even the simplest of the existing criteria. Worse yet, each of these criteria is itself incomplete in that it fails to encompass many of the possible risks that must ultimately be addressed. Unfortunately, previous attempts to define criteria specifically for voting systems [Sal88, Sha93, FEC, NYC87] are also incomplete. However, the risks lie in the inherent unrealizability of the criteria as well as in the incompleteness of those criteria.

ELECTRONIC VOTING CRITERIA

Generic voting criteria are suggested here as follows:

System integrity. The computer systems (in hardware and system software) must be tamperproof. Ideally, system changes must be prohibited throughout the active stages of the election process. That is, once certified, the code, initial parameters, and configuration information must remain static. No run-time self-modifying software can be permitted. End-to-end configuration control is essential. System bootload must be protected from subversion that could otherwise be used to implant Trojan horses. (Any ability to install a Trojan horse in the system must be considered as a potential for subverting an election.) Above all, vote counting must produce reproducibly correct results.

Data integrity and reliability. All data involved in entering and tabulating votes must be tamperproof. Votes must be recorded correctly.

Voter anonymity and data confidentiality. The voting counts must be protected from external reading during the voting process. The association between recorded votes and the identity of the voter must be completely unknown within the voting systems.

Operator authentication. All people authorized to administer an election must gain access with nontrivial authentication mechanisms. Fixed passwords are generally not adequate. There must be no trapdoors --- for example, for maintenance and setup --- that could be used for operational subversions.

* **System accountability.** All internal operations must be monitored, without violating voter confidentiality. Monitoring must include votes recorded and votes tabulated, and all system programming and administrative operations such as pre- and post-election testing. All attempted and successful changes to configuration status (especially those in violation of the static system integrity requirement) must be noted. This capability is similar to that of an aircraft flight recorder, from which it is possible to recover all important information. Furthermore, monitoring must be nonbypassable --- it must be impossible to turn off or circumvent. Monitoring and analysis of audit trails must themselves be nontamperable. All operator authentication operations must be logged. ([Gre93] analyzes accountability further.)

* **System disclosability.** The system software, hardware, microcode, and any custom circuitry must be open for random inspection at any time (including documentation), despite cries for secrecy from the system vendors.

* **System availability.** The system must be protected against both accidental and malicious denials of service, and must be available for use whenever it is expected to be operational.

* **System reliability.** System development (design, implementation, maintenance, etc.) should attempt to minimize the likelihood of accidental system bugs and malicious code.

* **Interface usability.** Systems must be amenable to easy use by local election officials, and must not necessitate the on-line control of external personnel (such as vendor-supplied operators). The interface to the system should be inherently fail-safe, fool-proof, and overly cautious in defending against accidental and intentional misuse.

* **Documentation and assurance.** The design, implementation, development practice, operational procedures, and testing procedures must all be unambiguously and consistently documented. Documentation must also describe what assurance measures have been applied to each of those system aspects.

Other lower-level criteria from the TCSEC are also applicable, such as trusted paths to the system, trusted facility management, trusted recovery, and trusted system distribution. All of the above criteria elements require technological measures and some administrative controls for fulfillment. The following item requires primarily nontechnological factors.

* **Personnel integrity.** People involved in developing, operating, and administering electronic voting systems must be of unquestioned integrity. For example, convicted felons and gambling entrepreneurs are suspect.

The above set of skeletal criteria is by no means complete. There are many other important attributes that election computing systems need to satisfy operationally. For example, Saltman [Sal88] notes that voting systems must conform with whatever election laws may be applicable, the systems must not be shared with other applications running concurrently, ballot images must be retained in case of challenges, pre- and

post-election testing must take place, warning messages must occur during elections whenever appropriate, would-be voters must be properly authorized, handicapped voters must have equal access, it must be possible to conduct recounts manually, and adequate training procedures must exist.

REALIZABILITY

No criteria can completely encompass all of the possible risks. However, even if we ignore the incompleteness and imprecision of the suggested criteria, numerous intrinsic difficulties make such criteria unrealizable with any meaningful assurance.

System trustworthiness

* **Security vulnerabilities** are ubiquitous in existing computer systems, and also inevitable in all voting systems --- including both dedicated and operating-system-based applications. Vulnerabilities are particularly likely in voting systems developed inexpensively enough to find widespread use. Evidently, no small kernel can be identified that mediates security concerns, and thus potentially the entire system must be trustworthy.

* **System operation** is a serious source of vulnerabilities, with respect to integrity, availability, and in some cases confidentiality --- even if a system as delivered appears to be in an untampered form. A system can have its integrity compromised through malicious system operations --- for example, by the insertion of Trojan horses or trapdoors. The presence of a **superuser** mechanism presents many opportunities for subversion. Furthermore, Trojan horses and trapdoors are not necessarily static; they may appear only for brief instants of time, and remain totally invisible at other times. In addition, systems based on personal computers are subject to spoofing of the system bootload, which can result in the seemingly legitimate installation of totally bogus software. Even in the presence of cryptographic checksums, a gifted developer or subverter can install a flaw in the system implementation or in the system generation. Ken Thompson's Turing-Lecture stealthy Trojan horse technique [Tho84] illustrates that no modifications to source code are required.

* **System integrity** can be enhanced by the use of locally nonmodifiable read-only and once-writable memories, particularly for system programs and preset configuration data, respectively.

* **Data confidentiality, integrity, and reliability** can be subverted as a result of compromises of system integrity. Nonalterable (e.g., once-writable) media may provide some assistance for integrity, but not if the system itself is subvertible.

* **Voter anonymity** can be achieved by masking the identity of each voter so that no reverse associ ____ can be made. However, such an approach makes accountability much more difficult. One-way hashing functions or even public-key encryption may be useful for providing later verification that a particular vote was actually recorded as cast, but no completely satisfactory scheme exists for guaranteeing voter anonymity, consistency of the votes tabulated with respect to those cast, and correct results. Any attempt to maintain a bidirectional on-line association between voter and votes cast is suspect because of the inability to protect such information in this environment.

* **Operator authentication** must no longer rely on sharable fixed passwords, which are too easily compromised in a wide variety of ways. Some other type of authentication scheme is necessary, such as a biometric or token approach, although even those schemes themselves have recognized vulnerabilities.

* **System accountability** can be subverted by embedded system code that operates below the accounting

layers, or by low-layer trapdoors. Techniques for permitting accountability despite voter anonymity must be developed, although they must be considered inherently suspect. Read-only media can help ensure nontamperability of the audit trail, but nonbypassability requires a trusted system for data collection. Accountability can be subverted by tampering with the underlying system, below the layer at which auditing takes place. (See also [Gre93].)

* **System disclosability** is important because proprietary voting systems are inherently suspect. However, system inspection is by itself inadequate to prevent stealthy Trojan horses, run-time system alterations, self-modifying code, data interpreted as code, other code or data subversions, and intentional or accidental discrepancies between documentation and code.

System Robustness

* **System availability** can be enhanced by various techniques for increasing hardware-fault tolerance and system security. However, none of these techniques is guaranteed.

* **System reliability** is aided by properly used modern software-engineering techniques, which can result in fewer bugs and greater assurance. Analysis techniques such as thorough testing and high-assurance methods can contribute. Nevertheless, some bugs are likely to remain.

* **Use of redundancy** can in principle improve both reliability and security. It is tempting to believe that checks and balances can help satisfy some of the above criteria. However, we rapidly discover that the redundancy management itself introduces further complexity and further potential vulnerabilities. For example, triple-modular redundancy could be contemplated, providing three different systems and accepting the results if two out of three agree. However, a single program flaw (such as a Trojan horse) can compromise all three systems. Similarly, if three separately programmed systems are used, it is still possible for common-fault-mode mistakes to be made (there is substantial evidence for the likelihood of that occurring) or for collusion to compromise two of the three versions. Furthermore, the systems may agree with one another in the presence of bogus data that spoofs all of them. Thus, both reliability and security techniques must provide end-to-end protection, and must check on each other.

In general, Byzantine algorithms can be constructed that work adequately even in the presence of arbitrary component failures (for example, due to malice, accidental misuse, or hardware failure). However, such algorithms are expensive to design, implement, and administer, and introduce substantial new complexities. Even in the presence of algorithms that are tolerant of n failed components, collusion among $n+1$ can subvert the system. However, those algorithms may be implemented using systems that have single points of vulnerability, which could permit compromises of the Byzantine algorithm to occur without n failures having occurred; indeed, *one* may be enough. Thus, complex systems designed to tolerate certain arbitrary threats may still be subvertible by exploiting other vulnerabilities.

* **Interface usability** is a secondary consideration in many fielded systems. Complicated operator interfaces are inherently risky, because they induce accidents and can mask hidden functionality. However, systems that are particularly user-friendly may be even more amenable to subversion than those that are not.

* **Correctness** is a mythical beast. In reliable systems, a probability of failure of $10^{**}(-4)$ or $10^{**}(-9)$ per hour may be required. However, such measures are too weak for voting systems. For example, a one-bit error in memory might result in the loss or gain of $2^{**}k$ votes (for example, 1024 or 65,536). Ideally, numerical errors attributable to hardware and software must not be tolerated, although a few errors in reading cards may be acceptable within narrow ranges. Efforts must be made to detect errors attributable to

the hardware through fault-tolerance techniques or software consistency checks. Any detected but uncorrectable errors must be monitored, forcing a controlled rerun. However, a policy that permits any detected inconsistencies to invalidate election results would be very dangerous, because it might encourage denial-of-service attacks by the expected losers. Note also that any software-implemented fault-tolerance technique is itself a possible source of subversion.

System Assurance

* **High-assurance systems** demand discipline and professional maturity not previously found in commercial voting systems (and, indeed, not found in most commercial operating systems and application software). High-assurance systems typically cost considerably more than conventional systems in the short term, but have the potential for payoff in the long term. Unless the development team is exceedingly gifted, high-assurance efforts may be disappointing. As a consequence, there are almost no incentives for any assurance greater than the minimal assurance provided by lowest-common-denominator systems. (See [Neu93] for a discussion of some of the implications of attaining high assurance.) Furthermore, even high-assurance systems can be compromised, via insertion of trapdoors and Trojan horses, and operational misuse.

CONCLUSIONS

The primary conclusion from the above discussion of realizability is that certain criteria elements are inherently unsatisfiable with assurance that can be attained at an acceptable cost. Systems could be designed that will be operationally less amenable to subversion. However, some of those will still have modes of compromise without any collusion. Indeed, the actions of a single person may be sufficient to subvert the process, particularly if preinstalled Trojan horses or operational subversion can be used. Thus, whereas it is possible to build better systems, it is possible that those better systems can also be subverted. Consequently, there will always be questions about the use of computer systems in elections. In certain cases, sufficient collusion will be plausible, even if one is not a confirmed conspiracy theorist.

There is a serious danger that the mere existence of generally accepted criteria coupled with claims that a system adheres to those criteria might give the naive observer the illusion that an election is nonsubvertible. Doubts will always remain that some of the criteria have not been satisfied with any realistic measure of assurance and that the criteria are incomplete:

* Commercial systems tend to have lowest common denominators, with numerous serious security flaws. Custom-designed systems may be even worse, especially if their code is proprietary.

* Trojan horses, trapdoors, interpreted data, and other subversions can be hidden, even in systems that have received extensive scrutiny. The integrity of the entire computer-aided election process may be compromisible internally.

* Operational misuses can subvert system security even in the presence of high-assurance checks and balances, highly observant poll watching, and honest system programmers. Registration of bogus voters, insertion of fraudulent absentee ballots, and tampering with punched cards seem to be ever-popular techniques in low-tech systems. In electronic voting systems, dirty tricks may be indistinguishable from accidental errors. The integrity of the entire computer-aided election process may be compromisible externally.

* The requirement for voter confidentiality and the requirement for nonsubvertible and sufficiently complete end-to-end monitoring are conceptually contradictory. It is essentially impossible to achieve both

at the same time without resorting to complicated mechanisms, which themselves may introduce new potential vulnerabilities and opportunities for more sophisticated subversions. Monitoring is always potentially subvertible through low-layer Trojan horses. Furthermore, any technique that permitted identification and authentication of a voter if an election were challenged would undoubtedly lead to increased challenges and further losses of voter privacy.

* The absence of a physical record of each vote is a serious vulnerability in direct-recording electit. (DRE) systems; the presence of an easily tamperable physical record in paper-ballot and card-based systems is also a serious vulnerability.

* Problems exist with both centralized control and distributed control. Highly distributed systems have more components that may be subverted, and are more prone to accidental errors; they require much greater care in design. Highly centralized approaches in any one of the stages of the election process violate the principle of separation of duties, and may provide single points of vulnerability that can undermine separation enforced elsewhere in the implementation.

There is a fundamental dilemma to be addressed.

* On one hand, computer systems can be designed and implemented with extensive checks and balances intended to make accidental mishaps and fraud less likely. As an example pursuing that principle, New York City [NYC87] is attempting to separate the processes of voting, vote collection, and vote tallying from one another, with redundant checks on each, hoping to ensure that extensive collusion would be required to subvert an election, and that the risks of detection would be high; however, that effort permits centralized vote tallying, which has the potential for compromising the integrity of the earlier stages.

* On the other hand, constraints on system development efforts and expectations of honesty and altruism on the part of system developers seem to be generally unrealistic, while the expectations on the operational practice and human awareness required to administer such systems may be unrealistic.

We must avoid lowest-common-denominator systems, instead trying to approach the difficult goal of realistic, cost-effective, reasonable-assurance, fail-safe, and nontamperable election systems.

Vendor-embedded Trojan horses and accidental vulnerabilities will remain as potential problems, for both distributed and centralized systems. The principle of separation is useful, but must be used consistently and wisely. The use of good software engineering practice and extensive regulation of system development and operation are essential. In the best of worlds, even if voting systems were produced with high assurance by persons of the highest integrity, the operational practice could still be compromisible, with or without collusion. Vigilance throughout the election process is simply not enough to counter accidental and malicious efforts that subvert the process. Some residual risks are inevitable.

ACKNOWLEDGMENT

REFERENCES

[Dug88] R. Dugger. Annals of Democracy (Voting by Computer). New Yorker. November 7, 1988.

[FEC] Federal Election Commission guidelines. %voluntary standards.

[Gre93] G.L. Greenhalgh. Security and Auditability of Electronic Vote Tabulation Systems: One Vendor's Perspective. *Proc. 16th National Computer Security Conference,* NIST/NCSC, Baltimore MD, September 1993.

[Mer93] R. Mercuri. Threats to Suffrage Security. *Proc. 16th National Computer Security Conference,* NIST/NCSC, Baltimore MD, September 1993.

[NeuPar89] P.G. Neumann and D.B. Parker. A Summary of Computer Misuse Techniques. *Proc. 12th National Computer Security Conference,* NIST/NCSC, Baltimore MD, pp. 396--407, October 1989.

[Neu90] P.G. Neumann. Risks in Computerized Elections (Inside Risks). *Comm. ACM 33,* 11, p. 170, November 1990.

[Neu93] P.G. Neumann. Myths of Dependable Computing: Shooting the Straw Herrings in Midstream. *Proc. 8th Annual Conf. on Computer Assurance (COMPASS '93),* June 1993.

[NYC87] Electronic Voting System. Request for Proposal, Appendix G, Security and Control Considerations. New York City Board of Elections, New York City Elections Project, September 1987.

[Sal88] R.G. Saltman. Accuracy, Integrity, and Security in Computerized Vote-Tallying. NBS (now NIST) special publication, 1988.

[Sal93] R.G. Saltman. Assuring Accuracy, Integrity and Security in National Elections: The Role of the U.S. Congress. Position paper from *Computers, Freedom and Privacy '93,* pp. 3.8--3.17, March 1993.

[Sha93] M. Shamos. Electronic Voting --- Evaluating the Threat. Position paper from *Computers, Freedom and Privacy '93,* pp. 3.18--3.25, March 1993.

[Tho84] K. Thompson. Reflections on Trusting Trust. *Comm. ACM, 27,* 8, pp. 761--763, August 1984.

Rebecca Mercuri's Statement on Electronic Voting

Copyright © 2001 by Rebecca Mercuri   All Rights Reserved.

mercuri@acm.org   http://www.notablesoftware.com
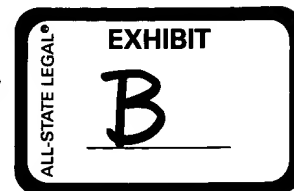
I am adamantly opposed to the use of any fully electronic or Internet-based systems for use in anonymous balloting and vote tabulation applications. The reasons for my opposition are manyfold, and are expressed in my writings as well as those of other well-respected computer security experts. To briefly summarize my opinion (based on a decade of research) on this matter I state the following:

- Fully electronic systems do not provide any way that the voter can truly verify that the ballot cast corresponds to that being recorded, transmitted, or tabulated. Any programmer can write code that displays one thing on a screen, records something else, and prints yet another result. There is no known way to ensure that this is not happening inside of a voting system.

- Electronic balloting systems without individual print-outs for examination by the voters, do not provide an independent audit trail (despite manufacturer claims to the contrary). As all voting systems (especially electronic) are prone to error, the ability to also perform a manual hand-count of the ballots is essential.

- No electronic voting system has been certified to even the lowest level of the U.S. government or international computer security standards (such as the ISO Common Criteria or its predecessor, TCSEC/ITSEC), nor has any been required to comply with such. Hence, no current electronic voting system has been verified as secure.

- There are no required standards for voting displays, so computer ballots can be constructed to be as confusing (or more) than the butterfly used in Florida, giving advantage to some candidates over others.

- Electronic balloting and tabulation makes the tasks performed by poll workers, challengers, and election officials purely procedural, and removes any opportunity to perform bipartisan checks. Any computerized election process is thus entrusted to the small group of individuals who program, construct and maintain the machines.

- Although convicted felons and foreign citizens are prohibited from voting in U.S. elections (in many states), there are no such laws regarding voting system manufacturers, programmers and administrative personnel. Felons and foreigners can (and do!) work at and even own some of the voting machine companies providing equipment to U.S. municipalities.

- Encryption provides no assurance of privacy or accuracy of ballots cast. Cryptographic systems, even strong ones, can be cracked or hacked, thus leaving the ballot contents along with the identity of the voter open to perusal. One of the nation's top cryptographers, Bruce Schneier, has recently expressed his concerns on this matter, and has recommended that no computer voting system be adopted unless it also provides a physical paper ballot perused by the voter and used for recount and verification.

- Internet voting (whether at polling places or off-site) provides avenues of system attack to the entire planet. If the major software manufacturer in the USA could not protect their own company from an Internet attack, one must understand that voting systems (created by this firm or others) will be no better (and probably worse) in terms of vulnerability.

- Off-site Internet voting creates unresolvable problems with authentication, leading to possible loss of voter privacy, vote-selling, and coersion. Furthermore, this form of voting does not provide equal access for convenient balloting by all citizens, especially the poor, those in rural areas not well served by Internet service providers, the elderly, and certain disabled populations. For these reasons, off-site Internet voting systems should not be used for any government election.

It is a known fact that the computer industry does not have the capability, at present, to assure a safe, reliable election using only electronic devices. Thorough investigation of vendor claims (such as those performed by New York City on DRE products), and failures of performance in actual elections, have demonstrated the existence of major flaws. Communities that rely on promises of security and accuracy when purchasing such systems, run the severe risk that they will administer an election whose results may someday be contested -- but they will not be able to provide an independent audit which can ascertain the content of the true ballots cast. In short, Florida all over again. Even worse, system defects may be revealed years after an election, making all earlier results questionable.

It is therefore incumbent upon all concerned with elections to REFRAIN from procuring ANY system that does not provide an indisputable paper ballot which can be checked by the voter visually before deposit and used by the election board in the case of recount.

Florida's voting systems were in the news again last month. A 10 September primary election marked the state's first large-scale roll-out of tens of thousands of sleek new touch-screen voting machines, the cornerstone of Florida's plan to resolve the problems of the 2000 U.S. presidential election by replacing many of their punch-card and other older machines.

The confusing butterfly ballots and hanging chads of two years ago are indeed gone. But in their place voters found touch-screen devices that didn't work properly or, in some cases, at all. A few machines in Miami-Dade County reset themselves while voters were trying to vote. Precincts in Palm Beach County reported problems activating some of the elec-

US $2–$4 billion will be spent in the United States and Canada to update voting systems during the next decade.

It seems plausible to imagine that computerized methods for ballot casting and tabulation could alert the voter to mistakes—for example, by flagging overvoting, when more candidates are chosen than is allowed, and by reducing undervoting, when some selections are skipped. New vote-tallying systems, which count the marks made on ballots, should be faster, more accurate, and cost-effective, and better able to prevent certain types of tampering (such as ballot-box stuffing) than older products.

And voting online might enable citizens to vote even if they are unable to get to the polls. Yet making these methods work right turns out to be considerably more difficult than originally thought.

A Better Ballot Box?

New electronic voting systems pose risks as well as solutions

BY REBECCA MERCURI
BRYN MAWR COLLEGE

tronic cards used to authenticate the voters. Even mark-sense ballots designed to be read by optical scanners proved troublesome. In Union County many votes had to be hand-counted because the optical scanning system reported all votes as being cast for just one party's candidate.

Will the November general elections in Florida be less chaotic? To judge from these primaries—and from Palm Beach County's municipal elections in March, which had a number of electronic voting problems as well—probably not. Using the new machines, it is still possible to inadvertently cast a ballot for a candidate that the voter never intended to select. Will the results be more reliable? There will simply be no way to ever know, because the new equipment does not make an independent recount possible.

Around the globe, election officials are examining technologies to address a wide range of such voting issues. The problems observed in the November 2000 election accelerated existing trends to get rid of lever machines, punch-cards, and hand-counted paper ballots and replace them with mark-sense balloting, Internet, and automatic teller machine (ATM) kiosk-style computer-based systems [see table, p. 48]. An estimated

As it turns out, many of the voting products currently for sale provide less accountability, poorer reliability, and greater opportunity for widespread fraud than those already in use. These problems result from an underlying fundamental conflict in the construction of electronic voting (e-voting) systems: the simultaneous need for privacy and auditability, which is the ability, when necessary, to recount the votes cast. Privacy is critical to a fair election, necessary to prevent voter coercion, intimidation, and ballot-selling. But maintaining the voter's privacy precludes the use by computer-based products of standard audit and control practices: logging transactions and identifying them from end to end. In other words, the privacy constraint directly conflicts with the ability to audit the ballot data.

For the system to work, there must be a way to backtrack vote totals from actual ballots that come from (and must be independently verified by) legitimate voters voting no more than once. In turn, the ballot must in no way identify or be traced back to the voter after it is cast. These constraints, many experts say, cannot be mutually satisfied by any fully automated system.

Such problems plague all electronic voting products, whether kiosk systems, where voters go to a polling station, or Internet-based, where voters can submit a ballot from their homes, offices, or any site connected to the global network. Unlike

automated teller machines at banks, where videocameras are used to deter theft, receipts are issued, cash provides a physical audit mechanism, and insurance covers losses, the privacy requirement means that analogous checks and balances cannot be employed to protect ballots in e-voting systems.

Internet voting is further flawed because authentication of the voter must be performed by the same system that records the ballots, and this compounds the auditability and privacy problems.

Just verifying a person's right to vote is difficult. Civil rights groups have objected, for example, to the use of bio-identification through fingerprints and retinal scans, fearing that the data will be used for criminal investigations or other purposes. Alternative log-in mechanisms, like personal identification numbers or smart cards, are not viable since they can be easily transferred, sold, or faked. To quote cryptographer Bruce Schneier, founder of Counterpane Internet Security Inc. (Cupertino, Calif.): "A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created in the history of computers."

Electronic voting offers fewer problems when used for such things as shareholders' meetings, public policy initiatives, award nominations, opinion surveys, and school, club, and association elections. These systems will have different requirements for security and auditability, depending upon their use. Web-based shareholder balloting has grown in popularity despite fears of computer security experts. Peter Neumann, principal scientist of SRI International's Computer Science Laboratory (Menlo Park, Calif.), is one expert who for years has warned that "the Internet is not safe for elections, due to its vast potential for disruption by viruses, denial-of-service flooding, spoofing, and other commonplace malicious interventions." Such a problem occurred in April 2002, when the financially troubled media conglomerate, Vivendi Universal (Paris), fell victim to a hacking attack that caused the ballots of some large shareholders to be counted as abstentions. Fortunately, since shareholder balloting is not anonymous (votes must be identified with their owners during tabulation), this particular breach was detectable.

● To Ensure an Accurate Ballot

The Mercuri Method allows voters to check that their votes will be recorded accurately by requiring that electronic voting machines be modified to generate paper ballots. Such a system does not exist, but could be created by machine manufacturers.

● In the proposed system, a voter, Zelda, votes on a touch-screen machine.

●● The system records Zelda's vote electronically, but the definitive record is a paper ballot, which the system prints and displays behind a glass or plastic panel.

●●● Zelda reviews the printed ballot. If it does not represent her choices, she calls an election official who voids the ballot. She votes again, and once she approves the ballot, it drops into a ballot box for later tallying. Ballots may be optically scanned or hand-counted.

The difficulties with Internet security are insurmountable, yet government officials have announced online voting initiatives in many countries, including France, Germany, Australia, and Estonia. In the United States, Internet voting was used in the Alaska and Arizona primaries in 2000, and some military personnel tested an experimental product later that year. The lure of increased voter participation seems to be the primary motivation for deploying Internet voting systems, although actual elections have demonstrated that such improvement may be relatively insignificant.

For example, last March, in local UK elections where online balloting was available, some districts saw a modest (1–5 percent) increase in voter turnout, while others did poorly. David Allen, a proponent of e-voting and spokesman for the St. Albans Labour party, was quoted as saying: "We were extremely disappointed with the results, turnout was worse than last year. People were actually deterred by the systems."

things worse. You have to trust the computer to record the votes properly, tabulate the votes properly, and keep accurate records."

In truth, no manner of self-reporting by the e-voting system is sufficient to ensure that intentional tampering, equipment malfunction, or erroneous programming has not affected the election results. Neither is any examination of the system, before, during, or after the election, no matter how thorough, sufficient to assert that such problems did not exist. This is due, in part, to the inherently insoluble task of making certain that computer-based products do not contain unknown additional features.

Trusting trust

Almost 20 years ago, in a classic paper, "Reflections on Trusting Trust," Ken Thompson, a co-inventor of the Unix operating system at AT&T's Bell Laboratories, said: "You can't trust code that you did not totally create yourself....No amount of

On the Road Toward Electronic Balloting

Twenty years ago, three-fourths of all U.S. counties voted by paper ballot or mechanical lever machines. In 2000, fewer than a third of them used such methods. Optically scanned, mark-sense ballots had the largest share (40.2 percent of counties), with direct-recording electronic devices (8.9 percent) moving up. Punch card machines still maintained a hold (19.2 percent) but will drop off sharply.
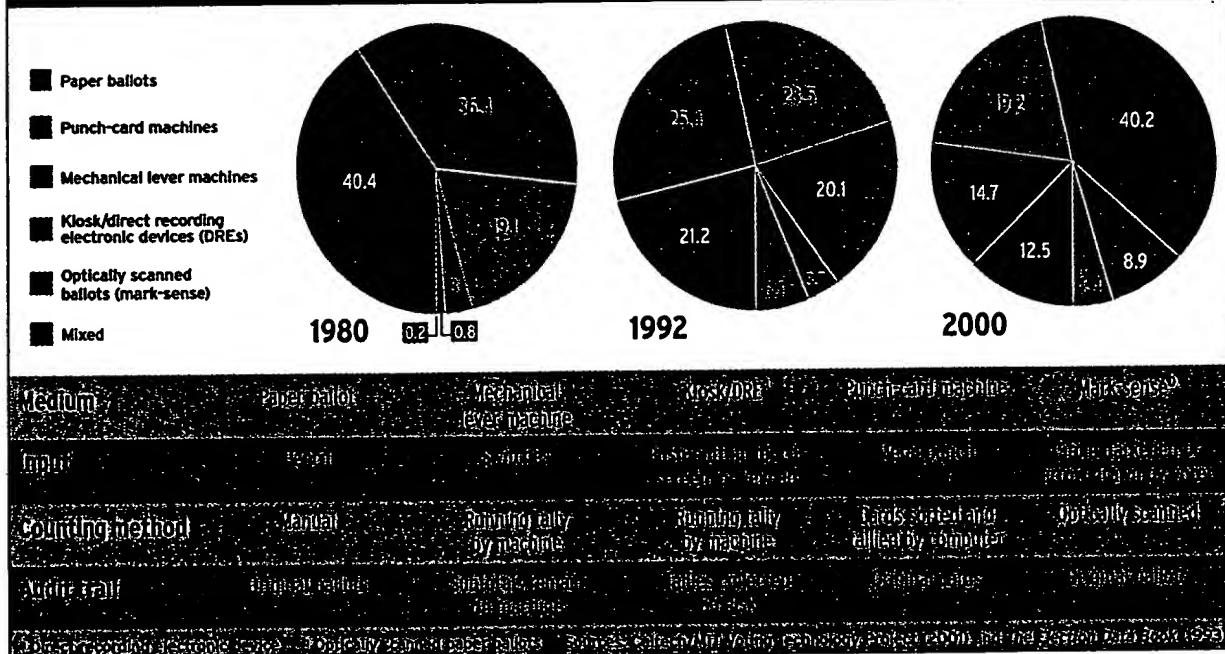
Despite manufacturers' statements to the contrary, it is beyond the scope of present computer science and engineering principles to design a fully electronic, self-auditing voting system that sufficiently guarantees that all ballots are recorded and tallied in accordance with the voters' intentions. Even so, e-voting systems are often viewed as an improvement by some communities, such as those in Florida or Brazil (in 2000, the first to use fully computerized balloting nationwide) that have suffered from earlier election scandals or difficulties. But reliance on this type of so-called fail-safe system design is risky, as Counterpane's Bruce Schneier has noted: "Computerized voting machines, whether they have keyboard and screen or a touch-screen ATM-like interface, could easily make

source-level verification or scrutiny will protect you from using untrusted code....A well-installed microcode bug will be almost impossible to detect." This computational reality has profound implications for voting systems. Whereas earlier technologies required that election fraud be perpetrated at one polling place or machine at a time, the proliferation of similarly programmed e-voting systems invites opportunities for large-scale manipulation of elections.

Appropriate system testing, though, often reveals the presence of some of these flaws, so organizations such as the IEEE, the U.S. National Institute of Standards and Technology, and the U.S. Federal Election Commission have begun

efforts to formulate criteria for the evaluation of voting equipment. It should be noted that in the United States, elections are not run by the federal government but by states and local jurisdictions. Therefore, the legislative bodies responsible for the administration of elections would need to mandate the use of these standards.

But even when standards and testing have been applied to voting systems, problems have occurred. This is due, at least in part, to the fact that all brand-new equipment is still being inspected to measure up to the Federal Election Commission's (now outdated) 1990 guidelines. The aforementioned Palm Beach County, the same locale plagued by the chad-recount issue in November 2000, purchased 3800 new touch-screen voting machines from Sequoia Voting Systems (Oakland, Calif.) for US $14.5 million in 2002.

These machines were first used in March for various municipal elections, with problems that presaged the September primary election debacle. When the results were tallied, a large number of undervotes was indicated. Two losing candidates, the former Boca Raton Mayor Emil Danciu, whose race showed an 8 percent undervote, and Albert Paglia, who lost a runoff election (in which there were only two candidates) by only 4 votes with a 3 percent undervote, both decided to contest the election results.

Many voters came forward with sworn affidavits describing anomalies at their polling places. These problems included difficulties in selecting candidates ("When I touched the screen, nothing happened"), the machine "freezing up" while voting, voting-authorization smart cards being rejected, and manipulation of voting machines (such as turning it off and on, or pressing buttons on the back panel) by poll workers during the balloting session.

The Danciu case proceeded to Palm Beach County's 15th Circuit Court with a request for an independent evaluation of the voting equipment used in the election. There, Teresa LePore (Palm Beach County supervisor of elections, and a defendant in the case) revealed that the county's purchase contract included trade-secret clauses that would make it a third-degree felony to disclose details of the specifications or internal functioning of the machines. LePore also testified that she couldn't understand why anyone would want to take apart the machines since, in her words, "there's not much inside there."

Further, she noted that the vendor would void the warranty on the machines if they were opened for inspection. Effectively, any independent verification of proper operation was limited to examining the outside of the box.

Subsequently, Judge John D. Wessel allowed Danciu only "a walk-through inspection of all equipment used in the election." It was discovered that though automated procedures were used for pre-election testing, only votes for the first candidate in each race had been checked via the machine's screen. Since Danciu was listed third, the actual election may have been the first time an attempt was made to activate his ballot position. After the election, the machines switched into a mode to prevent ballots from being cast, so it was impossible to ascertain (without an internal examination) whether malfunction or poor programming resulted in improper logging of votes for any of the candidates. The matter remains under investigation.

Beyond all of this, the machines produced by various vendors and adopted for use in Florida, California, and other localities suffer from additional major flaws. It is possible, for example, to activate a candidate position that has not been touched by pressing the screen in two positions simultaneously. Unintended voting choices—exactly the problem that precipitated Florida's election troubles back in 2000—were thus not prevented by this new equipment.

Trade secrecy, usability, privacy, security, and other inherent computer issues result in a dangerous "trust us" mentality on the part of manufacturers

Even more risky is the fact that at least one machine's firmware, that of the Sequoia Edge, can be reprogrammed through a port on the voting machine kiosk. Although this port is "secured" during the voting session by a flimsy, numbered, plastic tab, it is exposed after the election, providing essentially no protection against reprogramming.

E-voting products from other companies have also proved problematic. The systems involved in the 10 September voting snafus in Miami-Dade and Broward counties were from Election Systems & Software Inc. (Omaha, Neb.). Problems included machines that took three times longer than expected to boot up, that reset themselves spontaneously, and, in one precinct, that apparently failed to record about 1800 votes.

Recently, an evaluation performed by the University of Maryland on a system being considered by four Maryland counties—the AccuVote-TS touch-screen system from Diebold Election Systems Inc. (Canton, Ohio)—produced evidence of a digital divide. Individuals familiar with computers found the system easier to use than those with less computer experience. The study also revealed reliability problems during the system's first use in an April school board election when smart cards for authenticating voters had been produced to incorrect specifications, delaying voting at some sites. Nevertheless, last May, Diebold won a $54 million contract from the state of Georgia, which plans to use the systems in all 159 counties.

Trust, but verify

The combination of the lack of standards, legislative loopholes, trade secrecy, usability problems, privacy, security, and other inherent computer issues results in a dangerous "trust-us" mentality. Transparency in the process is essential, not only to provide auditability, but also to enhance voter confidence.

This can be provided, quite simply, through the use of a voter-verified physical audit trail for use in recounts.

A method of voting described by this author over a decade ago, referred to as the Mercuri Method, requires that the voting system print a paper ballot containing the selections made on the computer [see illustration, p. 47]. This ballot is then examined for correctness by the voter through a glass or screen, and deposited mechanically into a ballot box, eliminating the chance of accidental removal from the premises. If, for some reason, the paper does not match the intended choices on the computer, a poll worker can be shown the problem, the ballot can be voided, and another opportunity to vote provided.

At the end of the election, electronic tallies produced by the machine can be used to provide preliminary results, but official certification of the election must come from the paper records. Since the ballots are prepared by computer in machine- and human-readable format, they can be optically scanned for a tally, or hand-tabulated for a recount. After the election, yet other entities (such as the League of Women Voters or a news organization like Reuters) can verify the ballots using their own scanning equipment, if the format is produced in a generic way.

This type of system is cost-effective. No longer must blank ballots be prepared in advance, as with mark-sense or other paper-based voting systems. Incidentally, mark-sense products—pre-printed ballots with circles or ovals that a voter fills in with a pencil or pen—do provide a physical record that is available for recount. They have the lowest undervote rate of all the computerized tabulation systems, according to a number of studies, including one by the Caltech/MIT Voting Technology Project [see "On the Road Toward Electronic Voting," p. 48].

One e-voting system, still only at a trial stage, from Populex Systems (West Dundee, Ill.), is similar to the Mercuri Method. As company founder Sanford Morganstein puts it, "The count is not something that's kept in a computer, but one that is tangible, that you can look at." Nonetheless, it differs in an important respect: voters use a touch screen to generate a printed ballot that contains only a bar code to indicate the votes. Thus, the system is open to vote tampering, according to Doug Jones, a computer science professor at the University of Iowa who examines e-voting technologies, since many voters won't check that the bar code matches their choice.

According to Jones, an election could be rigged by altering at random, say, one ballot in 100, enough to swing many close elections. "If only 1 voter in 100 bothers to check, that means that only 1 in 10 000 will find an error," Jones says. And who's to know that the bar-code reader hasn't been programmed to misread ballots? Hence, the Mercuri Method requires a human-readable plain text printout.

Besides its utility in recounts, the fact that the voter sees the final ballot on the screen as well as on paper has been shown to help voters catch their own mistakes. Visually impaired or illiterate voters can be allowed to use voice-feedback scanners to read the paper ballot, so they would not be disenfranchised by this process.

The Mercuri Method recount concept has been incorporated into recent voting legislation reforms (including some in Florida, California, and Maryland) that require the voting systems to produce paper audit trails. Brazil will use the method for 3 percent of its voting systems in an upcoming election.

Although some vendors, such as Avante Systems (Princeton, N.J.), have started to incorporate voter-verifiability into their products, the largest companies have oddly interpreted these laws to mean that audit trail printing can be done from the internally recorded ballots after the election. Their claim is that cryptography and redundancy will be used to secure the data. But these techniques are insufficient to ensure end-to-end correctness, since voters cannot verify that the ballots produced are indeed the ones they cast. Furthermore, data can be corrupted (intentionally or accidentally) early in the process, resulting in stored information that seems correct, but may not be.

Cryptography can, though, be effectively used along with a voter-verifiable ballot to prevent ballot-box stuffing, and to make certain that the paper tallies match the electronic


Palm Beach County's infamous butterfly ballot confused some voters in November 2000. Intending to pick the second choice in the left-hand column [Gore/Lieberman], they used the second circle from the top, which was actually a vote for the topmost choice in the right-hand column [Buchanan/Foster].

results. David Chaum, a Palo Alto, Calif., cryptologist who, 20 years ago, invented electronic cash, has a technique that provides the best of all possible worlds: a computer-generated, voter-verified physical ballot that also gives the voter a receipt that can be used to determine that his or her vote was tabulated correctly, without revealing its contents.

One drawback of Chaum's method is that to demonstrate that the votes are tallied correctly requires a lot of math. As a result, it is difficult to explain to election officials, poll workers, and voters how it establishes the correctness of the balloting and tabulation process. But it gives a glimpse of the type of voter-verifiable systems that may be used for future elections.

An observer of voting technology once remarked: "If you think technology can solve our voting problems, then you don't understand the problems and you don't understand the technology." Computerization alone cannot improve elections. Those designing and those buying election systems must be aware of their inherent limitations, mindful of the sometimes conflicting needs for privacy, auditability, and security in the election process, and willing to seek out-of-the-(ballot)-box solutions. ●

Steven M. Cherry, *Editor*

verifiedvoting.org
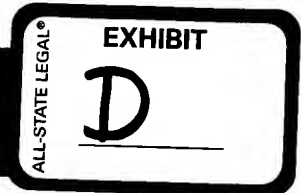
Frequently Asked Questions about DRE Voting Systems

David L. Dill, Rebecca Mercuri, Peter G. Neumann, and Dan S. Wallach

Section 1: Paper vs. Computers

- 1.1. What is a DRE?
- 1.2. Why are computer scientists upset by DRE voting systems?
- 1.3. What exactly is a "voter-verifiable audit trail" and why must we have it?
- 1.4. Then how can DRE vendors improve their systems?
- 1.5. If DRE systems have paper, then what's the point of the computer?
- 1.6. What if the paper and the computer disagree on the vote totals?
- 1.7. Won't the paper produced by such a computer be just as subject to problems as traditional punch-card or optical-sense systems?

Section 2: Software Quality

- 2.1. DRE vendors say their software has been thoroughly tested. Isn't that good enough?
- 2.2. DRE vendors claim that preserving the secrecy of their proprietary technology gives them an important hedge against being compromised.
- 2.3. The vendors have to escrow the source code of their systems with the Secretary of State's office. Doesn't this solve the problem?
- 2.4. Don't the Federal and State certification processes make sure the machines are secure?
- 2.5. Why are electronic voting machines different from your bank's automated teller systems?
- 2.6. Why are electronic election machines different from safety-critical systems with stringent requirements for reliability (for example , airplane flight-control systems)?

Section 3: Practical Advice

- 3.1. We are mandated to replace our existing voting system, but no existing replacement is certified for our use that does what you suggest. What should we do?
- 3.2. How great are the risks of using DRE machines?
- 3.3. How do these risks compare with systems based on paper ballots?
- 3.4. Have problems in DRE machines been seen in real elections?
- 3.5. What about accessibility for voters with disabilities?

Section 1: Paper vs. Computers

1.1. What is a DRE?

DRE stands for "Direct Recording Electronic" voting machine. As the name suggests, the voter directly enters the votes, which are recorded electronically. Almost all touch screen voting machines are DREs, although there are other DREs that have knobs or switches instead of touch screens.

`↑ BACK TO TOP`

1.2. Why are computer scientists upset by DRE voting systems?

Computer scientists, as well as voters, are upset by paperless DRE voting systems because we know that even a beginning programmer can write code that displays votes one way on a screen, records them another way, and tallies them yet another way. This can happen for a variety of reasons, including software and hardware errors, or "hacks" installed into the voting machines. These problems can occur even when voting machines have been thoroughly inspected and tested. DRE systems experienced a number of problems already in the 2002 elections, and we see this only as the tip of the iceberg.

`↑ BACK TO TOP`

1.3. What exactly is a "voter-verifiable audit trail" and why must we have it?

To have confidence that votes are being correctly recorded, we need to guarantee that voters will directly see a physical object that shows their vote. Voters must be confident that this physical object cannot be thrown out or changed by the voting system. Of course, once a vote has been cast, the voter's anonymity must be preserved, and this physical object becomes the final record of the voter's intent. The voter cannot keep any proof of how they voted.

Traditional manual elections that use paper ballots and marking pens, as well as newer optical scan systems (i.e., mark-sense or bubble form), have the audit trail we want. Voters mark the paper, can hold it in their hands, can verify it, and can then put it in a ballot box. We also like DRE voting systems that print a paper ballot which the voter can see and approve. Paperless DRE systems tell voters to just "trust us" that the system will work. That diminishes voter confidence.

`↑ BACK TO TOP`

1.4. Then how can DRE vendors improve their systems?

DRE voting systems need to use printer attachments to produce a printed paper ballot of the voter's selections, printed in the voter's native language. The voter can read and verify that his or her intent is represented on the paper ballot. The computer-printed paper ballot should be treated with all the care of traditional paper ballots. The ballots are, of course, anonymous, and election officials keep them securely in ballot boxes.

In a DRE system with a paper component such as this, *the vendor's software no longer needs to reach unattainably high levels of quality and security*, so long as it works well enough to produce the paper ballot. Either the voter is happy with the paper output or not. If not, then it's a spoiled ballot, and traditional procedures can be applied to guarantee that the voter's spoiled ballot is not placed in the final ballot box.

`↑ BACK TO TOP`

1.5. If DRE systems have paper, then what's the point of the computer?

Computer-based systems can offer significant improvements in human-factors, making voting accessible to voters with visual or motor impairments as well as supporting a number of different languages. DRE systems can help prevent undesirable over-voting and under-voting. They can also support elections with more races and even with non-traditional voting systems like approval voting or instant run-offs. Furthermore, the use of computers allows election workers to quickly tally

computer-based voting records. However, the paper-based records will be more accurate and will need to be tallied as well.

`[↑ BACK TO TOP]`

1.6. What if the paper and the computer disagree on the vote totals?

If there is a difference between counts produced from the paper ballots and purely electronic counts from the voting machines, paper ballots should generally take precedence as the paper ballots have been seen and verified by voters, whereas the electronic counters inside the voting machines have not.

Of course, in the event that the election administration had problems (for example, misplacing paper ballot boxes), then the electronic counts may in such special circumstances be considered to be better than nothing at all from a given precinct. Whenever paper ballots exist, their tally will be the most dependable information available.

`[↑ BACK TO TOP]`

1.7. Won't the paper produced by such a computer be just as subject to problems as traditional punch-card or optical-sense systems?

Luckily, no. There will be no "chads" on the paper that need to be punched and no bubbles for a voter to fill in. Computer printouts can be easily read, both by people and by other computers, providing two possible avenues for counting paper ballots. Furthermore, cryptographic techniques (i.e., secret computer codes) can be applied by the DRE system to make it essentially impossible for voters to insert fake ballots.

`[↑ BACK TO TOP]`

Section 2: Software Quality

2.1. DRE vendors say their software has been thoroughly tested. Isn't that good enough?

It is not enough to show that a system "seems to work." We know that the testing of existing DRE systems has already missed some impressive flaws. For example, Diebold voting systems in Georgia would "lock up" after a few hours use, despite being tested in a mock election with more votes than a typical machine got during the real election.

Second, testing for security problems, especially if they were intentionally introduced and concealed, is basically impossible. Consider the cute surprises inserted by programmers into commercial software that are triggered by obscure combinations of commands and keystrokes, called "Easter eggs." These routinely slip through vendor's quality assurance testing, including the amazing flight simulator that is hidden in <u>Microsoft Excel '97</u>. An Easter egg slipped into a voting program would never be detected. If the Easter egg allowed a voter to modify the votes inside the machine, it could change the whole election.

`[↑ BACK TO TOP]`

2.2. DRE vendors claim that preserving the secrecy of their proprietary technology gives them an important hedge against being compromised.

This argument is generally called "security through obscurity" and has been disproven time and time again. Adversaries will always be able to get voting machines to tear apart and study. They may

even be able to design "hacks" that modify voting machines after the machines are in use.

Computer security researchers accept that, for a system to be secure, it must be designed to resist adversaries who know every detail about its inner workings. Furthermore, we have seen too many cases where a vendor claims its software is secure when it turns out to be full of holes. Currently, the results of voting system certification tests are kept secret and vendors hide their hardware and software from other independent scrutiny by aggressive use of trade secret agreements. Security claims need to be independently audited, and, even if the source code is not available in public, the detailed security audits should be public, to make a strong argument that the voting system actually works.

`↑ BACK TO TOP`

2.3. The vendors have to escrow the source code of their systems with the Secretary of State's office. Doesn't this solve the problem?

It doesn't seem to help at all. In fact, it's not clear that there are any circumstances where the code can be examined. In cases where clearly flawed elections have been challenged in some states, the vendors and courts have refused to let independent experts look at the source code. Furthermore, the detailed reports from the certification authorities have also been protected by trade-secrecy, so even in a court proceeding it is impossible to check whether the equipment has been properly configured, and whether testing has been sufficient to assure confidence in its accuracy and reliability.

`↑ BACK TO TOP`

2.4. Don't the Federal and State certification processes make sure the machines are secure?

A: No. The NASED (National Association of State Election Directors, the organization that oversees certification to Federal requirements) and California state certification processes are considerably weaker than other accepted standards for the security of computer-based products. Security-critical systems for the Department of Defense, for example, must meet the more stringent standards overseen by National Institute of Standards and Technology (NIST), such as the International Standards Organization (ISO)'s Common Criteria. Many other computer vendors, such as health care, voluntarily apply the NIST standards to their products, but to date, no electronic voting system has been certified under the NIST programs. (Some may have received ISO 9000 certification, but this is largely meaningless in the context of security.) The Help America Vote Act requires NIST work to develop a real standard (the FEC recommendations are not a standard, and require adoption by the states, only 2/3 of which have done so) for voting systems, but this work has not yet been funded, so an enforceable US standard for design, construction, and testing of election equipment does not yet exist. All current (and for the forseeable future) voting product "testing" under the NASED program is paid for by the vendors, performed in secrecy, and detailed result reports are not released for public scrutiny.

`↑ BACK TO TOP`

2.5. Why are electronic voting machines different from your bank's automated teller systems?

The ATM systems have all sorts of internal auditing, and they provide you with a paper record of your transaction that you can verify on the spot. If there is a discrepancy, you can immediately go into the bank and have it resolved. If your monthly statement shows transactions that you never made, you can get your bank to fix them. ATM systems also include cameras that can be used to identify criminals or to prove that a genuine customer was using the ATM. Banking systems are not anonymous, as elections are required to be. Also banks are insured for losses (and there are

considerable losses at ATMs), while elections are not insured. Election systems are thus
significantly more difficult to design and build than ATM systems.

In fact, <u>serious security problems</u> have recently been found with bank ATMs.
`[↑ BACK TO TOP]`

2.6. Why are electronic election machines different from safety-critical systems with stringent requirements for reliability (for example, airplane flight-control systems)?

The technical community is quite skilled at designing, building, testing, and evaluating computer
systems that must operate within highly reliable safety-critical applications such as real-time
aviation control, air-traffic control, space systems, health-care systems, and so on. It adds
significantly to the development costs, but those costs are generally justified by the clearly
recognized dangers from having these systems fail. DRE voting systems are not built with anything
approaching the level of care that goes into building safety-critical systems.

Furthermore, safety-critical systems are not generally designed to be secure against arbitrary misuse
or tampering. Election systems need to have the auditing and double-checking features found in
ATM systems combined with the reliability achieved in safety-critical systems. That's a tall order,
and current DRE systems give us no reason to believe they achieve this. However, if DRE systems
included paper ballot printing, as discussed above, this level of reliability would no longer be
necessary.
`[↑ BACK TO TOP]`

Section 3: Practical Advice

3.1. We are mandated to replace our existing voting system, but no existing replacement is certified for our use that does what you suggest. What should we do?

The authors of this FAQ do not wish to endorse any specific vendors, although we do point out that
both Avante's Vote-Trakker system and Advanced Voting Systems/Hewlett Packard's voting system
support voter-verified audit trails and are certified for use in California. If your municipality,
perhaps in collaboration with other municipalities around the U.S., demanded these features, other
vendors would certainly make them available in time to meet the March 2004 deadlines.

Major vendors Sequoia, Diebold, and ES&S have prototypes of voter-verifiable paper trails that can
be attached to their DRE machines. These systems still need to be certified, but that could probably
be completed in time for the 2004 elections.
`[↑ BACK TO TOP]`

3.2. How great are the risks of using DRE machines?

The risks of paperless DRE machines are large. Programming errors are an inevitable fact of life
given current technology. With these paperless DRE machines, there is nothing that can stop a
determined group from achieving large-scale election theft. We see no reason why major problems
will not occur, including obviously messed up elections, election of incorrect candidates, and,
certainly, disillusioned and disenfranchised voters.

*DRE voting systems that use voter-verified paper ballots have natural safeguards against numerous
forms of fraudulent election behavior.* Current DRE systems have no such safeguards.

3.3. How do these risks compare with systems based on paper ballots?

Of course, election problems and outright election-rigging have occurred with systems based on paper ballots. However, good election administration can minimize these problems. People understand paper ballots and know what measures need to be taken to keep them secure. Wide-scale tampering with paper ballots is quite difficult.

Computer-generated paper ballots can be **considerably better** than regular paper -- barcodes and cryptography can be added to the ballot to ensure that the paper was produced at the time of the election, and to prevent ballot-box stuffing. Hence, a "better ballot box" can be produced through the combination of computers with paper. With paperless DREs, the risk of a large scale computer error or fraud that can globally affect the outcome of an election is high. With paper ballots, each voter will know that their ballot has been cast correctly, and controls can be put into place that will ensure that the tabulation is performed publicly and properly.

With paperless electronic voting systems, there is a real risk that bugs or security holes could affect large numbers of votes, regardless of how well the election is run otherwise.

In a well-run election, paper ballots are vastly more reliable and secure than paperless DRE machines.

3.4. Have problems in DRE machines been seen in real elections?

Yes! Problems are routine. Disturbingly, no one gets to the bottom of some of them, even when the outcome of the election may have been affected. Here is one of many examples: In March 2002, in the city of Wellington, Florida, there was a runoff election between two candidates for a single office. The final tally was 1,263 to 1,259, but 78 ballots had no recorded vote. Elections Supervisor Theresa LePore put forth the implausible explanation that those 78 people came to the polls yet chose not to vote for the only office on the ballot!

Here is another example: In 2000, a Sequoia DRE machine was taken out of service in an election in Middlesex County, New Jersey, after 65 votes had been cast. When the results were checked after the election, it was discovered that, out of those 65 voters, *no votes* were recorded for the Democrat and Republican candidates for one office, even though 27 votes each were recorded for their running mates. A representative of Sequoia insisted that no votes were lost, and that voters had simply failed to cast votes for the two candidates. Since there was no paper trail, it was impossible to resolve the question.

These problems could have been avoided if the machines had printed voter-verifiable ballots. Voters would have caught missing votes when they inspected their paper ballots, and these ballots would have been available for counting when the election results were questioned.

3.5. What about accessibility for voters with disabilities?

See the Voting Accessibility Resources: Improving Voting Systems for Disabled People page.

[↑ BACK TO TOP]

Frequently Asked Questions (FAQ)

This document will be updated from time to time. The most recent version may be found at http://www.openvotingconsortium.org/faq.html

Updated: Monday, April 12, 2004

Table of Contents

Overview

1. What is the Open Voting system?

    The heart of democracy is voting. The heart of voting is trust that each vote is recorded and tallied with accuracy and impartiality.

    The Open Voting Consortium (OVC) is creating a trustworthy, cost effective, voter verifiable voting system using open source software components on industry standard computers.. A primary element of this Open Voting system is the use of software through which the voter creates a printed paper ballot containing his or her choices. Before casting his or her ballot the voter may use other, independently programmed, computers to validate that the ballot properly reflects the voter's choices. The paper ballot is cast by placing it into a ballot box. Once cast, that paper ballot is the authoritative record of the voter's choices for the election and for any recount of that election. Open Voting ballots are machine readable and may be tabulated (and verified and re-tabulated in the case of a recount) either by computer or by hand.

    Open Voting systems can be engineered to accommodate the special needs of those who who have physical impairments.

2. Why are people concerned?

    Voting is the foundation of democratic systems, whether those be direct or representative systems. There is no shortage of historical anecdotes of attempts to undermine the integrity of electoral systems. The paper and mechanical systems we use today, although far from perfect, are built upon literally hundreds of years of actual experience.

    There is immense pressure to replace our "dated" paper and mechanical systems with computerized systems. There are many reasons why such systems are attractive. These reasons include, cost, speed of voting and tabulation, elimination of ambiguity from things like "hanging chads", and a belated recognition that many of our traditional systems are not well suited for use by citizens with physical impairments.

    Many of us today have come to trust many of our financial transactions to ATM (automatic teller machines). The push for electronic voting machines has been a beneficiary of that faith in ATMs. However, we are starting to learn that that faith is unwarranted.

    First of all, ATM machines do fail and are often attacked. Those who operate ATM's usually consider the loss rate to be a proprietary secret. Banks are well versed in the actuarial arts and they build into their

financial plans various means to cover the losses that do occur. In more crude terms, it's only money.

Voting machines carry a more precious burden - there is no way to buy insurance or to set aside a contingency fund to replace a broken or tampered election.

There are several areas of concern regarding the new generation of computerized voting machines:

- ▶ No means for the voter to verify that his/her votes have been tallied properly.
- ▶ No means outside of the memories of the voting machines themselves to audit or recount the votes.
- ▶ Lack of ability to audit the quality of the software. Fortunately the widespread belief that "computers are always right" is fading. Our individual experiences with buggy software on personal computers and consumer products (e.g. the BMW 745I), software errors by even the best-of-the-best (e.g. NASA and the loss of the Mars Climate Orbiter), and the possibility that intentional software bugs can be hidden so deeply as to be virtually invisible (Ken Thompson's famous 1984 paper - Reflections on Trusting Trust) have all combined to teach us that we should not trust software until that trust has been well earned. And even then, we ought not to be surprised if unsuspected flaws arise.
- ▶ Vulnerability of the machines or of their supporting infrastructures to intentional attack or inadvertent errors.

The companies that produce voting machines have poured gasoline onto the smoldering embers of concern. Some of these products are built on Microsoft operating systems - operating systems that have a well earned reputation for being penetrable and insecure. And most of these companies claim that their systems are full of trade secrets and proprietary information and that, as a consequence, their internal workings may not be inspected by the public. In addition, these companies have frequently displayed a degree of disdain (in some cases disdain that takes the form of lawsuits) against those who are concerned about the integrity of these products. And finally, these companies themselves have frequently demonstrated an appalling lack of sophistication regarding the protection of their systems, procedures, and corporate computer systems. There is a widespread perception that these companies are more concerned about profits than about elections.

3. What are the core elements of the Open Voting system?

The Open Voting system is very much like a traditional system in which the voter enters the voting place, marks his or her choices onto a paper ballot, and inserts the ballot into a ballot box.

The Open Voting system applies computer technology to that traditional system. However, unlike some of the other computerized voting systems that change the basic nature of the traditional system, the Open Voting system applies computer technology only in a limited and conservative way.

The Open Voting system preserves the paper ballot. However, under the Open Voting system the voter marks the ballot using a computerized voting station rather than a pencil or colored marker. The ballot is printed in plain text that the voter can read. Voters have the opportunity to inspect the ballot to ensure that it properly reflects their choices.

The Open Voting system preserves the ballot box. Voters must insert their paper paper ballots into the ballot box. The Open Voting system ballots contain a bar code in addition to the plain text. This bar code makes it easy for the voting place workers to count the ballots when the ballot box is opened.

4. I've heard of Voter Verified Ballots, is this the same as Open Voting?

Voter Verified Voting is concerned that voting systems must record voters' choices onto a human readable media, usually paper, that can be reviewed by the voter to ascertain that his/her votes were correctly recorded, and also to serve as an independent, auditable record that may be used should a recount be necessary.

The OVC's Open Voting system is voter verifiable in all regards.

However, the OVC's Open Voting system addresses concerns in addition to voter verification and audit trails.

For more information of voter verification see VerifiedVoting.org.

TOP

Terminology

The words used to describe elections varies from jurisdiction to jurisdiction. Some of this difference is due to differences in custom, much of the difference comes from definitions cast into laws or from court decisions. See the United States Federal Election Commission's FAQ on Voting System Standards.

The Open Voting Consortium tries to use terminology in its most common forms.

1. **Voter** or **Elector**: For purposes of the Open Voting system, the terms *"voter"* and *"elector"* are synonymous. Both words refer to a person or persons who have the legal right to cast a vote in an election and who have come to an appropriate voting place or other official location in order to go through the process of voting in that election. The Open Voting system assumes that some procedural system is in place in that precinct or location to validate that a putative voter is in fact properly entitled to begin the voting process.

   The Open Voting system never "knows" the identity of any voter nor does the Open Voting system retain information that could be used to reveal the voter's choices.

2. **Election**: The OVC, and this FAQ, use the word *"election"* to mean the entire process in which one or more questions or contests are presented to voters and the choices of the voters obtained, tabulated, and archived in case of subsequent audit or recount.

3. **Contest**: A *"contest"* is a choice among designated alternatives (including "write in") that is presented to a voter. An example of a contest would be a list of candidates competing against one another for a particular office. The term contest also includes selections in which the voter may designate multiple choices, including selections in which the voter is asked to indicate a preferred priority or rank among the voter's selections.

4. **Question**: A *"question"* is a choice in which the user is asked to indicate a positive or negative vote, or no vote at all. An example of a contest would be the presentation of a bond measure for approval by the voters.

5. **Ballot**: A *"ballot"* is a document, electronic or paper, on which the voter's choices are recorded. In the Open Voting system, a ballot is a sheet of paper on which the voter's choices are printed by a *voting station*. In the Open Voting system, a ballot must be "cast" before those choices have effect.

   This ballot is intended to be easily read by the voter so that the voter may verify that his or her choices have been properly marked. In the Open Voting system the ballot also contains security markings as well as a bar code. That bar code mirrors the user's choices as expressed in the human readable portion of the ballot. (The Open Voting system allows the the voter to use ballot reader machines in order to verify that the bar code itself accurately mirrors the voter's choices.)

   The term *"ballot"* as used by the OVC is intended to identify with clarity and precision the paper produced when a voter uses an Open Voting system voting station. There are colloquial and imprecise uses of the term *"ballot"* that refer to the voting process as a whole or to a document presented to the voters on which are preprinted (or displayed) the entire set of contests and questions, including the list of candidates for each contest and summaries of the questions. The term *"ballot"* as used by the Open Voting system refers to the paper on which the voter's choices are recorded. A ballot must be "cast" in order to be tallied.

   Although the human readable text and the bar code on the ballot are intended to be equivalent, should a conflict occur, the human readable text ought to be given priority when trying to ascertain the voter's intent.

6. **Voting station**: A *"voting station"* is a computer that presents the contests (including the list of candidates) and questions to the voter. The voter interacts with the voting station in order to express the voter's choices (including write-ins.)

   Each voting station will produce a printed paper ballot that reflects the voter's choices. To complete the voting procedure the voter must <u>cast</u> his or her ballot into the <u>ballot box</u>.

   There will likely be various types of voting stations in order to accommodate the needs of physically impaired voters. For many voting stations this interaction may involve a touch screen, much like what is found on familiar automatic teller machines (ATM) and many DRE voting machines. Other voting stations may use voice technologies to accommodate sight impaired voters. In all cases the voting station produces a paper ballot on which are recorded the user's choices.

   The term *"voting station"* encompasses both the computer with which the voter interacts and the printer that writes the voter's ballot.

   Both the computer and the actual printer are low cost, readily available, industry standard, personal computer components. The only hardware element that might be unfamiliar to the ordinary personal computer user would be the touch screens and the anti-tampering physical container for the pieces of the voting station.

7. **Ballot reader**: A "*ballot reader*" is a computer that the voter may use to "read" the bar code on his or her ballot. The ballot reader will display, and if requested, will audibly articulate (through headphones) the choices that are recorded in the ballot's bar code. This gives voters, including voters who are sight impaired, the ability to verify the accuracy of their ballot.

   In order to counteract the risk of tampering, and also to detect software errors, the Open Voting system encourages the creation of ballot readers that use software from authors other than those who provide the software for the voting stations. This kind of cross-checking and mutual validation are one of the benefits that arise from the use of open source software in the Open Voting system.

8. **Ballot box**: The Open Voting system uses the familiar method of placing the paper ballot into a physically secure container. This container is the "*ballot box*". Different jurisdictions may have different rules regarding the physical construction of the box. For example, some ballot boxes may contain a distinct compartment into which spoiled ballots are deposited.

9. **Casting a vote**: In the Open Voting system, a ballot becomes an official statement of the voter's choices when the voter or a poll worker acting on behalf of the voter places the ballot into a ballot box. This is the same process used in many of today's voting systems around the world and in the United States. The actual mechanics of how a voter places his or her ballot into the ballot box, and the mechanical aspects of that voting box, will vary from jurisdiction to jurisdiction depending on local laws and customs.

10. **Recount**: The Open Voting system does not define how recounts or audits of an election may be performed. The Open Voting system does allow a jurisdiction to preserve the paper ballots and use those ballots to determine the intention of the voters.

    The Open Voting system builds several logs as it operates. These logs, which have been designed to preclude disclosure of any particular voter's choices, may be used to cross-check that the Open Voting system is working properly. These logs, if preserved by the jurisdiction holding the election, may be used after an election to isolate problem areas and to indicate how procedures might best be changed for the next election in order to avoid a recurrence of such problems.

11. **DRE** or **Direct Recording Electronic**: A DRE is an integrated electronic voting machine. DREs contain all voting functions - from presentation of the choices to the voter to collection, recording, and counting of the voters' choices.

    A DRE does not produce a ballot, the integrity of the count is based on the proper working of the DRE and the safe transfer of data from each DRE to the tabulation center. It is this lack of an independent permanent, voter verifiable record that has given rise to the concern for <u>voter verified</u> ballots.

    The <u>United States Federal Election Commission (FEC) informally defines DRE</u> as:

    > *The most recent configuration in the evolution of voting systems are known as direct recording electronic, or DRE's. They are an electronic implementation of the old mechanical lever systems. As with the lever machines, there is no ballot; the possible choices are visible to the voter on the front of the machine. The voter directly enters choices into electronic storage with the use of a touch-screen, push-buttons, or similar device. An alphabetic keyboard is often provided with the entry device to allow for the possibility of write-in votes. The voter's choices are stored in these machines via a memory cartridge, diskette or smart-card and added to the choices of all other voters.*

    > *In 1996, 7.7% of the registered voters in the United States used some type of direct recording electronic voting system.*

    The FEC has a more formal definition in section 1.5.3 of its <u>Voting System Standards</u>

    Some jurisdictions use the term DRE in slightly different ways.

    Note that DREs are a essentially "black boxes" - the voters input their choices and the final tally pops out the of the DRE at the end of the day.

    A lot of controversy has been raised about the trustworthiness of DREs. Because DREs are computers that combine all aspects of the voting process into a single, opaque black box, DREs are considered by independent experts to be vulnerable to a wide range of flaws, failure modes, and attacks.

12. **HAVA or Help America Vote Act of 2002**: Public Law 107-252. See URL: http://fecweb1.fec.gov/hava/hava.htm, (also 42 USC 15301 *et seq.*)

    HAVA is a United States law passed as a reaction to the election problems that occurred in the United States in year 2000. HAVA induces states to conduct elections according to certain standards. Under HAVA Federal funds are made available only to those states that conduct elections according to the standards that are elaborated in the statute

13. **Voter Verified Voting:** This is an issue akin to, but different from, Open Voting. Voter Verified Voting is concerned that voting systems, whether they be DREs or Open Voting systems, produce a human-readable, paper record of each vote that can be checked by the voter and used in the event of an audit or recount.

Open Voting systems are inherently voter verifiable; DREs are not.

See the VerifiedVoting web site at http://www.verifiedvoting.org/

TOP

Scenarios

1. Could you make a comparison between a legacy voting place and an OVC voting place?

Let us consider voting as it might have occurred in a Norman Rockwell style precinct in the mid twentieth century.

Legacy voting place: You would begin by entering the voting place and walking up to the poll workers sitting at a table. There you would sign your name in the precinct book and receive a preprinted sheet of paper (an "Australian Ballot") on which are listed the various contests, along with the names of all the candidates in those contests and a space for a write-in, as well as the various questions. Pre-printed circles or boxes would be present for the voter to mark his or her choices.

The voter would enter the voting booth and in the privacy of the booth the voter would mark his or her choices.

If the voter makes a mistake, the voter folds the spoiled ballot and takes it to the poll worker for a new blank ballot form. The poll worker would deposit the spoiled ballot into a special container.

After the voter has created his or her marked ballot the voter folds the ballot and brings it to the poll worker who assists in ensuring that the ballot is placed into the sealed, secure ballot box.

The voter then leaves the voting place.

At the end of the day, the ballot box is opened under the watchful eyes of the voting place workers and various observers. The ballots are taken out, inspected for damage, and counted. The totals are taken to the tabulation center where they are added with the counts from other voting places. The paper ballots themselves are preserved in case a recount is needed.

Open Voting System voting place: How is this different with the Open Voting system?

The steps in which the voter arrives at the voting place and signs in are unchanged.

Rather than being given a preprinted ballot form, the Open Voting system voter is given a smart card (like a credit card) that will activate a voting station. (In an alternative implementation, rather than using a smart card, a poll worker may simply enable the voting station for one use.)

The voter would close the curtain on the voting station machine and would see a touch screen computer display, much like that on an automatic teller machine (ATM) or on a typical DRE. The screen would show the voter the various contests (including the candidates plus space for a write-in) and the various questions. The voter would make his or her choices. The voter would then indicate that he or she is finished at which time the voting station would print the paper ballot showing the voter's choices.

(voting station machines for people with physical impairments might use means other than touch screens. For example, a machine for people with vision impairments might use a machine equipped with headphones and an audio response capability.)

The voter places the printed ballot into a folder so that only the bar code is visible. (The bar codes are augmented by special data so that the poll workers can't easily read the voter's choices from the bar code.)

The voter would be able to visually inspect his or her yet uncast ballot and, if desired, could have the bar code interpreted visually (and also audibly via headphones) using a separate ballot reader.

If the ballot is in error, the voter brings the ballot to a poll worker who places it into a special container for spoiled ballots. The voter is given a new smart card and goes back to the voting station machine to again make his or her choices.

If the voter is happy with the printed ballot, the voter brings the ballot to a poll worker who helps the voter place the folder containing the ballot into the ballot box, thus casting the ballot.

As was the case with the Rockwell style voting place, at the end of the day the ballot box is opened before the poll workers and observers and the ballots counted using bar code readers.

The totals are accumulated in the tabulation center and the physical ballots preserved in case of a recount.

Conclusion: It is easy to see that there is a great deal of similarity between how we voted in the past and how we would vote using the Open Voting system. The Open Voting system only changes what is appropriate to change and retains many of the aspects that have helped us trust that our elections accurately reflect the choices of the voters.

2. Could you make comparison between a voting place using DREs and a voting place using OVC?

   TBD

3. How does the Open Voting system deal with write-in votes?

   The user interfaces on the Open Voting system give the voter the opportunity to indicate that he or she desires to make a write-in. The voter is then presented with a screen (or audio menu if appropriate) that may be used to enter the write-in name.

   The user interface is designed so that the voter can spell-out the write-in name by selecting characters from the screen; keyboard skills are not necessary.

4. Can the Open Voting system handle contests in which the voter selects more than one candidate?

   Yes.

5. Can the Open Voting system handle a variety of vote aggregation (counting) methods?

   Yes, the mechanisms used in the Open Voting system may be used with virtually all current and proposed systems of counting votes.

   Most of the Open Voting system is concerned with the mechanisms for displaying elections and contests to voters, for aggregating the voter's choices onto a printed ballot, for optionally user verification of that ballot, for casting the ballot, and accumulating an electronic form of that data for use by tabulation tabulation software. The actual tabulation software could be extended to handle any of the various proposed vote counting systems.

   Some of the proposed systems of counting votes are somewhat intricate and are beyond the scope of this FAQ.

   For descriptions and explanations of various systems of counting votes see:
   ▸ http://www.electionmethods.org/evaluation.htm
   ▸ http://lorrie.cranor.org/pubs/diss/node4.html#SECTION00310000000000000000

6. How do you prevent a voter from voting more than once?

   The same sign-in procedures that prevent a voter in a Legacy Precinct from voting more than once would apply to an Open Voting System Precinct.

7. How do you prevent a ballot from being counted more than once?

   As with a Legacy Precinct, proper procedures have to be in place to ensure that each ballot is counted once and only once. In addition, since the bar code on Open Voting ballot includes the ballot number, the bar code reader used to count the ballots can detect if a ballot is scanned more than once, and prohibit the ballot from being counted again.

8. How do you prevent a voter from overvoting (voting for more candidates than there are positions to be filled)?

   The user interface of the Open Voting system will not allow the voter to select more candidates than there are positions to be filled.

9. What sort of training will voting place workers need?

   Open Voting systems do not eliminate the need for trained voting place workers or for well designed procedures.

The OVC intends to maintain a dialog with public officials who run elections in order to ensure that Open Voting systems mesh well with existing training and procedures. It is expected, of course, that some changes in training and procedures will be necessary. The OVC does not anticipate that the cost of this training or the overhead of the procedures will be significantly different than for any other system of electronic voting.

TOP

Physical Components

1. **Are commodity PCs adequately reliable or powerful to use as voting machines?**

   Yes. Modern commodity personal computers, even ones that are a few years old, are enormously powerful once unburdened from all of the ancillary tasks that we typically load onto a personal computer.

   The primary difference between a typical personal computer and one used as a voting machine is that the computers used for voting must be physically protected from tampering. This is easily done by putting them into a locked container (with adequate ventilation.) Many DREs do exactly this.

   In addition, in the Open Voting system, there will be several types of voting machines. There will be multiple types of voting stations in order to accommodate the needs of physically impaired voters. And there will be ballot readers so that voters can verify the accuracy of their ballots. Each of these different machines will have some peripheral hardware not found on the typical personal computer. For example, voting stations may have touch screens. And ballot readers may have bar code readers. Many machines will have headphones for use by visually impaired voters.

2. **Does a voting station contain a hard disk?**

   Not necessarily. It is possible to construct a voting station so that it boots and runs from a CD-ROM that has been certified by the authority in charge of the election. Such CD-ROM based systems are quite common - for example take a look at the <u>Knoppix</u> version of Linux.

   Voting stations do maintain log files that record certain administrative and trouble-detection information - such as the number of voters who have used the machine and the number of ballot pages sent to the printer. The amount of data in such logs is small enough that they would easily fit onto a commodity USB flash memory ("thumb drive") device.

3. **What kind of printers can be used?**

   Any reasonable quality laser printer can be used. Ink jet printers may also be acceptable.

   The primary issue regarding printers is reliability, particularly with regard to paper handling.

   Lesser, but still important, concerns include accuracy of the registration, i.e. the placement of the printing on the paper.

4. **Is special paper necessary?**

   The Open Voting system does not require special paper.

   There are those who argue that the security of elections may be enhanced if ballots are printed on specially watermarked paper that is physically protected from use in any role but in elections or in a particular election. The counter-argument is that if such paper falls into the hands of a would-be penetrator, then its use would give a degree of credence to false ballots.

   The Open Voting system paper ballot contains a background image that is printed at the same time that the ballot is printed. The choice of image and its placement can be established shortly before the election, thus adding resistance to attempts to pre-print false ballots and bring them into the voting place.

5. **What if the paper jams in the voting station or if the printer runs out of ink or toner?**

   Through procedural means it is possible to reduce the chance that a printer will jam or run out of ink or toner. For example, as part of the preparation for an election, each printer should be loaded with fresh ink or a fresh toner cartridge. (It is unlikely that any single election will consume an entire fresh load of ink or toner.) Similarly, the paper used should be stored under conditions of reasonable temperature and humidity, even if the voting place itself might have suboptimal temperature and humidity.

However, Murphy's Law is ever-present - "If anything can go wrong, it will, and at the worst possible time."

The OVC believes that the best way to handle printer problems is for a poll worker to remove the printer from the voting station machine, place that printer into secure storage, and to install a replacement printer. The exact procedural steps for this are yet to be worked out. Of particular concern are the handling and privacy of any damaged ballot that might be in the printer as well as the disposition of any unused paper in the feed tray.

This procedure suggests that every voting place have spare printers. Fortunately, printers, particularly ink-jet printers, are becoming very inexpensive, are compact, and can be set up very quickly.

Most voting places will have a sufficient number of voting stations to accommodate peak demand. If a printer fails during off-peak hours then the voting station with the bad printer can be taken off-line until the voting administrators can bring a new printer to the voting place.

6. What about uninterruptible power supplies (UPS)?

The OVC believes that all electronic voting equipment, with the possible exception of high-current draw machines such as laser printers, should be protected by uninterruptible power supplies.

Low cost uninterruptible power supplies will only be able to cover power outages of short duration, typically an hour or less.

Good uninterruptible power supplies have means to indicate how much time is left before they go dark. Voting place workers should have procedures that instruct them what to do as the power goes out and as the time that the UPSs run out of power comes near. For example there may be instructions to turn off some of the machines (and unplug them) and only use the remaining machines until power is restored. If the running machines reach the end of their power then they can be turned off and the other machines activated. This has the effect of doubling resilience to a power failure.

Uninterruptible power supplies of good design do more than simply provide power when the lights flicker or go out; a good UPS protects the computer equipment from failure or errors caused by power surges and spikes caused by storms or electrical utility problems.

7. What happens if the power or a UPS does fail?

The printed paper ballot is the core record created and used in the Open Voting system. Paper ballots are not affected by power failures.

Should there be a power failure (or machine failure) during the voting, any yet-unprinted ballot will not be printed; the voter will have to wait until power is restored and once again make all of his or her choices. Any partially printed ballots are considered spoiled.

Unlike a DRE, a power failure in the Open Voting system introduces no ambiguity into the ballots; there are no hidden electronic counters that may or may not have been incremented as the power went out, and the voter can inspect the paper ballot before casting it into the ballot box.

TOP

Access For Voters With Disabilities

The OVC recognizes that voters with disabilities are full citizens who have a right to vote on equal terms with every other citizen.

1. How can a sight-impaired voter verify his or her vote on the OVC system?

Special voting stations can be equipped with headphones and audio-response software. The OVC is experimenting with user interfaces to make it easy for a sight impaired person to cast his or her vote.

Once a ballot is printed, and before it is cast, a sight impaired voter (or any voter for that matter) may take the ballot to a ballot reader machine and have the ballot read-back through headphones.

2. Can the Open Voting system accommodate voters in wheelchairs?

Yes. The touch screen used in the Open Voting system is typically used in a horizontal position. However, it is quite feasible to construct a voting booth in which that screen can be lowered to an acceptable height or rotated into a vertical position. It is also feasible to construct a flat screen that is cabled so that it may be used on the voter's lap.

3. **How adaptable is the Open Voting system?**

The Open Voting system is based on commercial off-the-shelf computer hardware, including displays, audio interfaces, and and human interface devices. The OVC recognizes that these are not yet all that they could be in the fullness of time.

The OVC hopes to extend and adapt the Open Voting system as these new interface devices arise.

The flexibility of voting systems is constrained by local law. The following describes the situation nicely:

Voting and ballots are governed by an astounding number of local regulations. So when the party is to the right, bolded, in a sans serif font two points smaller than the candidate name, that's because some law somewhere calls for it. The end result is that you can't do some fairly obvious things in the layout that would make the ballots more readable because it violates some rule. Of course, people are fighting to improve those rules, but OVC's job is to promote an open system that conforms to the election laws, not to change them.

TOP

The Ballot

1. **What, exactly, constitutes "the ballot" in the Open Voting system?**

In the Open Voting system, the ballot is a paper document that contains the voter's choices. This paper is generated by a printer attached to an Open Voting ballot marking machine used by the voter to make his/her choices for each of the various contests that have been placed before the voter in the election.

Many of these Open Voting ballot marking machines will use touch screen technology, as is found on Automated Teller Machines (ATMs) and other kinds of voting machines. Some of these Open Voting ballot marking machines will be designed for use by voters with physical impairments. In all cases, each Open Voting ballot marking machine will contain a printer that produces the actual paper ballot that contains the voter's choices.

The voter will take the ballot from the Open Voting ballot marking machine's printer. The voter may visually inspect the ballot and may also carry the ballot to a separate machine that will read-back the bar-code on the ballot. This read-back machine is present both to assist sight impaired voters and also to give voters the assurance that the bar-code on the ballot properly mirrors the human-readable text on the ballot.

The choices printed on this ballot do not constitute countable votes until the ballot is "cast" by placing it into a ballot box.

2. **What's the difference between a voter verified *ballot* and other voter-verified paper trails?**

As long as the law or regulation that establishes the voter-verified paper trail specifies that the voter-verified paper trail is to be used in the case of a manual recount and in mandatory random spot-checks of machine-produced vote tallies, then a voter verified ballot an a voter-verified paper train are basically the same.

The important points of any voter-verified system are:

▶ The voter has an opportunity to verify a tamper-resistant record of their vote.

▶ That record is used in the event of a manual recount.

▶ When machine-produced vote tallies are used, a random sample of machine tallies are compared to a manual count of those records.

▶ **What does a ballot look like?**
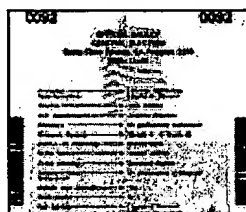
The ballot is a single sheet of paper, click the following links to see a sample - PDF | JPEG

Note that only the choices made by the voter are shown; a single sheet of paper can accommodate an election containing a large number of contests and questions, including the names of write-in candidates.

It is important to remember that the printed ballot is the summary of the choices

that the voter entered via a <u>voting station</u>. It is the voting stations that will present the full menu of potential choices and will do so through various user interfaces.

This sample shows how the Open Voting system ballot handles contests in which the voter selects a single candidate, no choice (i.e. the "Treasurer" contest and the "Health care initiative" question), contests in which the voter chooses multiple candidates (i.e. the "Cat Catcher" contest), contests in which the voter chooses a panel of candidates (i.e. the "President/Vice President" contest), and multiple candidates with ranking (i.e. the "County Commissioner" contest.)

Also note that the ballot contains bar codes that reflect these choices as well as various background and other markings that identify this as an official ballot and discourage forged ballots.

▶ What is the "privacy folder"?

The ballot contains the voters choices in two forms: a form that can be read by people and a a bar code that expresses those choices in a machine readable form.

The voting place workers may come in contact with the ballot should they be asked to assist a voter or if the ballot is spoiled. In order to protect voter privacy it is desirable to minimize the chance that a voting place worker might observe the voter's ballot choices.

A privacy folder is just a standard file folder with an edge trimmed back so that it reveals only the bar code part of a ballot. The voter is expected to take his/her ballot from the printer and place it into a privacy folder before leaving the voting booth. The ballot will be cast by placing it, still in its privacy folder, into the ballot box.

▶ What is the purpose of the number on the ballot?

TBD

▶ There's a bar code on the ballot - what does that bar code represent?

The bar code consists of several things:
▶ The selections made by the voter.
▶ Checksums to detect processing errors.
▶ Additional padding data to obscure the bar code so that poll workers, who will be able to see the bar code (but not the textual part of the ballot) will not be readily able to ascertain by eye what selections the voter made.

▶ What is the difference between a receipt and a ballot?

We speak of the Open Voting System creating a paper *ballot*, not a *receipt*, nor simply a "paper trail". In other words, in the Open Voting System, the printout from a voting station is the primary record of votes cast by a voter and is the ultimate statement of the voter's intent. Electronic records may be used for generating preliminary results more rapidly, but the paper *is* the vote.

Some writers discuss producing a paper receipt, which a voter might carry home with them, as they do an ATM receipt. There are two significant problems with this approach. In the first place, if we suppose that a voting station might have been tampered with and/or simply contain a programming error, it is not a great jump to imagine that it may print out a record that differs from what it records electronically. A receipt is a "feel good" approach that fails to correct the flaws of DREs.

But the second problem with receipts is even more fundamental. A voting receipt that can be carried away by a voter facilitates vote buying and vote coercion. An interested third party – even someone as seemingly innocuous as an overbearing family member – could demand to see a receipt for voting in a manner desired. In the Open Voting System, ballots must be placed into a sealed ballot-box to count as votes. If a voter leaves with an uncast ballot, even if she went through the motions of printing it at a vote station, that simply does not represent a vote that may be "proven" to a third party.

What some vendors refer to as a paper trail suffers from a weakness similar to the first problem paper receipts suffer. Under some such models, a DRE voting station might print out a summary of votes cast at the end of the day (or at some other interval). But such a printout is also just a "feel good" measure. If a machine software or hardware can be flawed out of malice or error, it can very well print a tally that fails to accurately reflect the votes cast on it. It is not paper that is crucial, but *voter-verifiability.*

▶ Some voting systems I have heard about use a system where a paper ballot is displayed under glass, but not handled directly by a voter. It seems like those systems would prevent ballot-stuffing, since voters do not have direct access to ballot-boxes. Why doesn't the Open Voting System use that approach?

There are several narrowly technical problems with "ballot under glass" systems. Such a system will almost inevitably be more expensive than one like ours that can use commodity printers. In addition, in order to

handle rejection of incorrect ballots, a "ballot under glass" system must have extra mechanical complexity, and thus additional opportunity for failure and tampering.

A more significant issue for "ballot under glass" systems is their failure to provide the quality of accessibility to vision-impaired or reading-impaired voters. Even ordinary sighted voters who happen to need reading glasses are likely to find "ballot under glass" systems more difficult to check than are Open Voting System printed ballots. Even if "ballot under glass" machines were to add provisions for audio feedback on final ballots, users are dependent on the very same machine that produced the ballot in the first place to provide the audio feedback. This may be a subtle point; experience over the centuries has taught us that the potential for tampering is reduced and security enhanced by having separate mechanisms. In this case, if a "ballot under glass" machine has been compromised, then why would one expect it to to perform an audio-read back that revealed that it has been penetrated and the vote changed? Potentially, a tampered-with machine could bias votes, but only for visually-impaired voters (still perhaps enough to change close elections). In contrast, the Open Voting System positively encourages third parties to develop software to assure the barcode encoding of votes matches the visibly printed votes – all voters are treated equally and all can verify their own ballots.

From a more sophisticated cryptology perspective, "ballot under glass" systems are likely to compromise voter anonymity in subtle ways. One of the issues the security researchers have considered is the possibility that sequential or time-stamp information on ballots could be correlated with the activity of individual voters. Even covert videotaping of the order in which voters enter a polling place might be used for such a compromise. Security experts are people who get paid to think about even the most nefarious attacks on systems, and voting is important enough to merit such paranoia.

While "ballot under glass" does indeed do a pretty good job of preventing ballot-box stuffing with forged physical ballots, this approach is not the only – nor even the best – technique to accomplish this goal. The Open Voting System is planning to incorporate cryptographic signatures and precinct-level customization of ballots that can convincingly prove that a challenged ballot actually was produced on authorized machines, at the proper voting place, rather than forged elsewhere. One such method is a simple customization of ballots accomplished by varying the page position of our ballot watermarks so that an outsider who wished to penetrate the system would have little time in which to brew-up a counterfeit ballot. In addition, a surprising amount of information can be subtly encoded by moving two background images relative to one another a few millimeters in various directions. Another method is to encode a cryptographic signature within the barcode on a ballot. (Care must be taken do do this in a manner that can be mathematically proven not to disclose anything about the individual voter who cast that vote, but simultaneously that cannot be forged without knowledge of a secret key.)

Professor Amit Sahai directs a Wiki (discussion site) where OVC developers analyze threat models at http://gnosis.python-hosting.com/cgi-bin/wiki.cgi

» See related question/answer.

TOP

Implementation

▶ How will the Open Voting System be implemented?

The software is primarily written in the Python language (version 2.3.)

The underlying operating system is Linux. (Presently we are using the Fedora and Suse distributions.)

It is expected that there will be at least two generations of software. First there will be the demonstration software that will server to convey the concepts and to improve understanding of how the final software should be structured. Then there will be the production software.

▶ Python?

Python is a small, but very powerful language.

It is an interpreted language, meaning that it is evaluated as it is executed. This makes Python very easy and flexible.

Python is a good language for prototype implementations. It is less clear whether Python is a good language for the non-prototype versions of the Open Voting system. Those systems will require certification.

Certification may be made more difficult by certain characteristics of Python. For example, unlike

compiled languages, certain types of Python programming errors, such as references to non-existent variables, are often not revealed until the erroneous code is encountered during execution.

Some or all of these concerns might be addressed by strict programming standards and by applying various tools, such as a Python compiler.

However, the OVC has yet to decide whether Python or some other language (such as Java) might serve as the foundation for the production versions of the Open Voting system.

▶ Linux?

The Open Voting system is constructed on Linux, or to be more accurate, it is constructed on one of the widely available Linux distributions.

The Linux kernel and the components of these distributions are open source. This means not only can they be inspected, but they can also be repaired if found to be flawed.

Linux distributions have become highly stable platforms; it is now quite common for Linux-based servers to run for years on end without intervention or fault.

Linux software, particularly the code in the kernel, is inspected by many people and tested by many more people, before it is released. The people who write, inspect, and test Linux code are people who have risen to these roles through a process of peer-selection. The brains, eyes, and hands that construct the Linux kernel are among the best in the industry.

Linux is free to use. This substantially reduces the cost of the components of the Open Voting system.

There are those who argue that Linux has higher life cycle costs than certain proprietary systems. While there may be some merit in those arguments in some limited cases, the experience of many of the members of the OVC has been to the contrary.

▶ Is the source code available

Yes. All source code will be made available. At the present time much of the code is on Sourceforge at http://sourceforge.net/projects/evm2003.

▶ Is the source code open source?

Yes. The Open Voting System will be distributed under a an extended form of the GPL. That extension is to simply require that the change history be maintained. This extension is intended to facilitate certification of the software by voting authorities by ensuring that the development history of the code is explicit and visible.

▶ Is a database used?

At the present time no formal database is being used. Databases tend to be complex and big. The data represented by a ballot is relatively small and simple. The Open Voting Consortium implementers felt that overall system reliability and maintainability, not to mention auditability and integrity, would be enhanced by avoiding the complexity of a full database and instead using simple XML based data files.

▶ Do you anticipate using diskless computers?

It is a goal of the Open Voting System to run on diskless computers. The system would boot from verifiable CD-ROMs in much the same way as Knoppix. Results would be accumulated on a redundant set of USB memory devices and CD-ROM burners.

This approach not only reduces the possibility of tampering or hardware failure, but it also gives county election officials the ability to prepare boot disks specifically tailored for each voting place. In addition it would reduce the technical expertise required of the voting place staff.

▶ What about using thermal printers and roll paper rather than commodity printers and standard paper?

We have heard statements that thermal printers and roll paper are more reliable than commodity printers. This may be true. However, it is presently the feeling of the Open Voting Consortium that with the price of commodity laser printers being so low that it is inexpensive for a voting place to have multiple spare printers that can be put into service should a printer jam or fail.

Another issue with thermal paper is its lack of longevity. Some jurisdictions require that all ballots be retained until at least the next election, and the archival quality of thermal paper leaves a lot to be

desired.

TOP

Security, Resiliency, Integrity, Reliability

▶ How does the Open Voting System deal with issues of security, resiliency, integrity, and reliability?

The Open Voting System is designed to deal with both intentional and accidental abuse from the outside and also to try to minimize or eliminate the effects of internal failures or errors.

The paper ballot produced by the Open Voting System is one of the core elements. The paper ballot, because it can be read by the voter represents a solid backstop against undetectable tampering of the machines through which the voter makes his or her selections. Similarly, the paper ballot is an archival quality document that can be examined at a later date to validate that the vote counting mechanisms performed accurately.

The Open Voting System, because it is based on open source software, can be inspected and tested by those who are skeptical by nature or those who are empowered to certify the system.

Moreover, because the system is open source, third parties or voters who might be suspicious of tampering are able to independently validate ballots and vote tallies. For example, one of the types of machine in the Open Voting System is one that allows a voter, particularly sight-impaired voters, to scan their yet-uncast ballot and have its contents read back (via headphones). A skeptical voter could, if allowed by the local law, bring a small portable implementation of this software with him or her into the voting place and scan his or her ballot for validity.

▶ Will voting machines be physically protected?

Yes. Although the Open Voting System uses commodity computers, it is expected that these will be enclosed in tamper resistant containers.

The staff at the voting place will, however, have to be alert to notice if someone is trying to break into those containers. And a procedure ought to be put into place to perform an inspection of the machines after the voting is closed.

▶ Will checksums and message digests be used to validate the correctness of software and data?

Yes. It is anticipated that boot disks will be protected from modification by content-digest algorithms such as MD5. These digests will be computed by the election officials who certify the boot media and will be checked as part of the voting place setup.

All voting data will be protected during transfer against modification or substitution by a combination of content-digest algorithms and cryptographic wrappers.

▶ What about the BIOS in the voting machines?

It is conceivable that someone could tamper with machine BIOS so that the Open Voting System software is loaded incorrectly and wrong results produced.

To do this would require a great deal of technical expertise as well as advance physical access to the voting machines. Because the computers used are commodity machines that could be put to other uses both before and after the election, such tampering would likely be noticed.

But even assuming that the BIOS were modified, the integrity of the election would be protected by the voter-verifiable paper ballot coupled with the fact that a successful attack would require that multiple machines be modified in a coordinated fashion.

▶ Are there risks that the Open Voting System does not address?

No system is perfect. And as technology moves forward new risks arise.

For example, the Open Voting System does not provide paper receipts showing a voter's choices that the voter may take away from the voting place. This is to protect against vote-selling and other forms of coercion. The Open Voting System however does not protect against the use of miniature cameras to record ballots.

Maintenance and Support

> ▶ How will counties get support and training in the use of the OVC software?

TBD

> ▶ What kind of maintenance does the Open Voting system require?

TBD

TOP

Comparisons With Other Systems .
This section will be rewritten.

> ▶ How does the Open Voting system compare with other voting systems?

TBD

TOP

The Demonstration
> ▶ When was the first demonstration?

The first public demonstration was held on April 1, 2004 at the Santa Clara County (California) county building.

Future demonstrations are being planned.

> ▶ What was demonstrated?

Four components were demonstrated:

> ▶ **Ballot marking machine with printer and full vision graphical user interface:** This is a touch-screen voting mechanism that results in a printed ballot.

> ▶ **Ballot marking machines with printer and vision impaired interface:** This is an audio system that allows sight impaired voters to make their choices. The voter wears headphones. The ballot is read to the voter and the voter makes his or her selections by pressing keys. Again this results in a printed ballot.

> ▶ **Ballot Vocalization Application:** This is an audio system that reads-back the paper ballot to the voter. It consists of a computer with a barcode scanner. This computer will enunciate the selections that are represented on the ballot so that any voter, and particularly vision impaired voters, may verify that their ballot correctly reflects their choices.

> ▶ **Reconciliation Application:** This system gathers the data from the cast and spoiled ballots, from integrity logs made by the voting machines, and from other sources (such as the roster of voters who came to the voting place), validates it, reconciles it, and produces results after the voting place closes.

TOP

Economics
> ▶ How much do DREs cost?

Initial costs: Direct Recording Electronic voting equipment is being sold for between $3,000 and $7,000(US) depending on the manufacturer and options which may be offered. Printer options for voter verification are rumored to range from $500(US) to $1,200(US).

Recurring costs: TBD

Support costs: Several DRE products are based on Microsoft operating systems and may use Microsoft or other proprietary applications in the DREs and in the tabulation systems. There will almost certainly be a degree of labor cost associated with keeping that software up to date with security and other patches, there also may be licensing costs to maintain the licenses for that software and to remain supported by the vendor.

▸ How much do Open Voting systems cost?

Initial costs: TBD

Because Open Voting systems are constructed using industry standard platforms (i.e. PC's), and because the computing demands placed on those platforms are low, a jurisdiction can deploy Open Voting systems using computers that are obsolete for office or educational use. This can greatly reduce system cost, vastly expand the pool of replacement units, and help reduce the cost of disposal of those otherwise obsolete computers.

Recurring costs:

Support costs: Open Voting systems will run on open source operating systems and use open source applications. Open source software will, like all software, require some labor to track and apply security and other patches. However there is no licensing cost to maintain licenses. There may be a hidden cost insofar as unless a contractual support relationship is established with a third party, there is no vendor contract that may be leveraged to coerce the resolution of problems or correction of software flaws. That cost may be mitigated, however, by the open source nature of the software that allows voting administrators across a variety of jurisdictions to mutually support one another.

TOP

Miscellaneous

▸ Do some places require, as part of recent voter verified ballot laws, that any ballot of paper that the voter verifies be protected behind a glass screen?

Yes, as part of the early reaction to DREs that did not allow voters to verify their votes and that did not create an independent audit record of the votes cast, some jurisdictions have mandated that such machines be equipped with printers. Sometimes those laws have imposed an additional requirement that the paper produced by the voting machine be protected by isolating it from the voter and making it visible only through a glass panel.

The Open Voting system, in the form described in this FAQ, does not provide this isolation between the voter and his or her ballot. The OVC does not consider this a weakness or a flaw. Moreover, the OVC has concern that isolated printers, particularly when coupled with means for the voter to reject the printed ballot, thus creating a spoiled ballot, could create mechanical and maintenance problems as well as adding considerable cost.

The OVC does plan, however, to review the system described in this FAQ to comprehend what changes would be needed to accommodate those jurisdictions that impose these kinds of requirements.

» See related question/answer.

▸ What is the effect of local laws on Open Voting?

In the United States, elections are governed by a combination of Federal and State (and local) law. The OVC is pleased to have among its founders people who have a great deal of expertise regarding the nuances and variations in election laws.

The OVC hopes that the Open Voting system that it proposes so closely models traditional paper ballot procedures that it will smoothly mesh with most voting laws and regulations. Because Open Voting systems are new, the OVC will not be surprised if there should occasionally be some issues that require localized adaptations.

TOP

Overview

▸ How do I contact the Open Voting Consortium?

The Open Voting Consortium web site is at http://www.openvoting.org/

▸ What is the scope of Open Voting?

Open voting affects democratic systems around the world. Much of the debate about computer based voting systems has been focused in the United States, mainly caused by election problems in year 2000 and the "Help America Vote Act" (HAVA).

▶ What is the Open Voting Consortium (OVC)?

The Open Voting Consortium is a California Nonprofit Mutual Benefit Corporation established December 12, 2003 with California corporation number C2567384.

The OVC's principal place of business, effective January 1, 2004, is:
Open Voting Consortium
9560 Windrose Lane
Granite Bay, California 95746
+1 (916) 791-0456 (voice)
+1 (916) 772-5360 (fax)

Official documents (We were assisted in the preparation of these documents by students at the University of the Pacific McGeorge School of Law under the direction of Professor Robert Hunt.):

▶ The Articles of Incorporation (draft) - http://www.openvotingconsortium.org/ad/OVC-articles-draft.pdf

▶ By-Laws: http://gnosis.python-hosting.com/cgi-bin/wiki.cgi?OpenVotingConsortiumBylaws

The OVC anticipates that it will apply to the United States Internal Revenue Service for 501(c)(6) status.

▶ Who are the people who comprise the Open Voting Consortium?

The Board of Directors (as of January 1, 2004) is comprised of:
▶ Douglas Jones
▶ Arthur Keller
▶ Alan Dechert
▶ Amit Sahai
▶ Peter Maggs

Officers of the OVC (as of January 1, 2004) are:
▶ Alan Dechert - President
▶ Douglas Jones - Vice-President, Chief Technology Officer, and acting Secretary
▶ Arthur Keller - Vice-President and Chief of Operations and Finance

▶ Can you join the Open Voting Consortium?

Like other consortia, the OVC will have various membership levels.

▶ How much will it cost to join the OVC?

The OVC is still in its formative stages; specific dollar amounts have not yet been determined..

▶ How is the Open Voting Consortium financed?

The OVC will be funded largely through membership fees.

▶ Will the OVC sell the machines or software?

No.

The OVC believes in open source mechanisms for the software that it creates. The OVC believes that Open Voting system software should be subject to inspection by the public. Furthermore, the OVC firmly believes that open source principles for Open Voting systems enhance resistance to inadvertent errors and to intentional tampering by enabling the creation of independent implementations that allowing for better audits and cross checking.

TOP

Reference Materials

▶ Voting and Elections (http://www.cs.uiowa.edu/~jones/voting/) by Douglas W. Jones, The University of Iowa - This page is full of in depth material about voting history and technology.

▶ United States Federal Election Commission (FEC) - http://www.fec.gov/

- ▶ Voting System Standards - http://www.fec.gov/pages/vss/v1/v1s1.htm
- ▶ Terms and Frequently Asked Questions- http://voter.browndogs.org/terms.html by the Voting Machine Study Group, edited by Charlie Strauss
- ▶ "Help America Vote Act" (HAVA) - http://fecweb1.fec.gov/hava/hava.htm
- ▶ Voter Verified Ballots - http://www.verifiedvoting.org/
- ▶ Electronic Voting Hot List (http://lorrie.cranor.org/voting/hotlist.html) by Lorrie Cranor - This list contains a comprehensive list of pointers to relevant materials.
- ▶ Voting methods:
  - ▶ http://www.electionmethods.org/evaluation.htm
  - ▶ http://lorrie.cranor.org/pubs/diss/node4.html#SECTION00310000000000000000
- ▶ Other forms of paper ballots:
  - ▶ David Chaum: Voting booths with secure receipts

verifiedvoting.org

E-Voting Misconceptions

This document debunks many of the common misconceptions about electronic voting machines.

Myth: A voter verifiable paper trail is a printer attached to a touch-screen machine.

Fact: A voter verifiable paper trail (VVPT, otherwise known as a "voter-verified paper ballot," or VVPB) is nothing more or less than a permanent paper record of the vote that the voter can check for accuracy (by some trustworthy method, such as visual inspection) before the vote is cast. The record must be deposited in a secure ballot box for use in a manual recount or audit.

This definition is quite broad, and encompasses "plain old paper ballots" that are manually marked and counted, central and precinct-based optical scan ballots that are hand-marked but read by computers, and printers on a touch-screen or other computerized input device.

At this time, the Verified Voting Foundation recommends precinct-based optical scan technology. It is widely used and proven in practice and studies have shown these systems to have lower residual vote rates (votes for too few or too many candidates) than e-voting machines.

Historically, the biggest problem with optical scan has been accessibility for people with certain disabilities, such as blindness, that make it difficult to vote a paper ballot. However, this situation has changed. New equipment is now coming on the market that provides an accessible computer interface to optical scan ballots (e.g., the AutoMark system being sold by ES&S). Some places also use low-tech tactile ballots for accessibility. For more information on voting machine accessibility, see our statement on disability access at http://www.verifiedvoting.org/article.asp?id=1875

Myth: Receipts will enable voters to prove how they voted to someone outside the polling place, enabling vote influencing or selling schemes.

Fact: This concern is based on a misunderstanding. Voter-verified paper ballots must be deposited in a secure ballot box in the polling place, even though some people call VVPBs "receipts." There is no more risk of vote selling with optical scan ballots or ballots printed on a touch-screen machine than with other kinds of ballots. There is much less risk of vote selling than with absentee ballots.

Myth: E-voting machines cannot be hacked because they are not connected to the Internet.

Fact: Computer systems can be hacked in many ways without using the Internet. Making systems secure against outsiders, such as voters and poll workers, is very hard, and, as multiple studies have shown, the current e-voting systems fail miserably. However, making them secure against INSIDERS, possibly even the programmers themselves, is close to impossible.

The way we make systems honest is to enable truly independent audits. Each voter should be able to check that his or her vote is recorded correctly, and it should be possible to count the paper ballots manually to double-check any machine counts.

Some e-voting machines are believed to have wireless connectivity that might enable Internet access with or without the knowledge of poll workers and election officials.

Myth: H.R. 2239 advocates "a return to flawed systems."

Fact: This is not the case. The Voter Confidence and Increased Accessibility Act (H.R. 2239) simply requires voter-verified paper ballots, as described above.

Paper systems are not "flawed." A 2001 Caltech/MIT study and several subsequent studies have found that paper ballot systems have lower error rates than all other voting methods, including direct recording electronic (DRE) machines.

Myth: Voter-verified paper trails "would force voters with disabilities to go back to using ballots that provide neither privacy nor independence, thereby subverting a hallmark of the HAVA legislation."

Fact: So far as we know, no one is proposing to suspend or delay the HAVA requirement that there be at least one accessible voting system in
each polling place by 2006.

Paper ballot systems can be made accessible in several ways: There is a touch-screen interface for optical scan ballots (described above); touch-screens that print paper ballots can also have equipment to read those ballots back to voters using an audio interface; "ballot on demand" systems that print blank optical scan ballots as needed in the polling places can also have accessible interfaces that allow voters to make their ions on the computer, then print out a ballot that is marked appropriately; and there are even low-tech ballot "tactile ballots" that have been used in Rhode Island and several countries to make optical scan systems accessible without computers.

Myth: The Technical Guidelines Development Committee of the Election Assistance Commission (EAC), not Congress, can "ensure the reliability of the computer technologies being employed in voting systems."

Fact: This is impossible, especially as applied to the next general election. The EAC Commissioners themselves were not appointed until December 2003, and to this day there is no Technical Guidelines Development Committee. Even if there were, the EAC is not required to produce guidelines until nine months after its members have been appointed.

Even if it released guidelines tomorrow, the guidelines are voluntary, as determined by HAVA's authors, and could be changed with the stroke
of a pen. Ironically, those who favor waiting for technical guidelines to be issued for a paper audit system are advocating the use of technology that has been shown to be error-prone and un-auditable.

Myth: "There has never been a documented case anywhere in the country where an electronic voting machine has produced an inaccurate tally of the votes."

Fact: This statement is misleading at best. There are many cases where e-voting machines appear to have RECORDED votes inaccurately, including the 2002 election in Wake County, North Carolina where 436 votes were lost because of a software bug.

The use of the word "tally" is perhaps a semantic trick, meaning that incorrectly recorded votes were then totaled

correctly. If so, it misses the point that the vote totals fail to represent how the voters voted.

For a catalog of the the e-voting miscounts and malfunction in recent elections, see http://www.verifiedvoting.org/resources/documents/ElectronicsInRecentElections.pdf (Adobe PDF format).

Myth: E-voting machines are not computers, so they are not subject to problems of computer security.

Fact: Florida Secretary of State Glenda Hood actually said this. It is a totally incorrect statement. The most widely used models machines have the same microprocessors that are used in PCs. By any reasonable definition, they are computers that execute computer programs, so they are subject to the same hardware and software bugs, and the same security issues, as all other computers. Just because they don't normally have a keyboard or mouse attached does not mean that they are not computers.

Myth: Printers are unreliable; VVPB printers will jam and/or run out of ink or paper, causing long lines at the polls.

Fact: High-reliability printers are available and deployed in many applications, e.g., ATMs, self-service boarding pass printers for airlines, etc., and printers print thousands of receipts everyday with little difficulty. While such VVPB printers might occasionally require attention by a poll worker, the same is true for e-voting machines.

Of course, optical scan machines don't require printers.

Myth: It just costs too much money to print paper ballots. E-voting will save money.

Fact: The purchase price of e-voting machines is three times as much as precinct-based optical scan. It will take at least 15 years of ballot printing costs to make up the difference. Also, the operational costs of e-voting machines are often underestimated. Some jurisdictions have found that they needed more poll workers to conduct an election with e-voting machines (e.g., San Diego needed twice as many!). There are increased costs for equipment maintenance and storage. Testing is more expensive, and so on.

Previous Page

[Issued to the press and handed out on the Capitol steps in Salt Lake City UT, JUL 13th, 2004]

Alan Dechert's statement

Thank you. I am glad to be here on this beautiful day in the beautiful State of Utah! I thank Utah Count Votes and Kathy Dopp for inviting me.

Four years ago, America learned there were some serious flaws in our voting system. Personally, I was embarrassed that my country--a country that prides itself as a champion of democracy and a champion of technology--was having so much trouble with such a basic thing as counting the votes.

I was one of those that jumped into the debate, determined to see the problems corrected. Four years later, we've made some progress but we still have a very messy situation on our hands. Mistakes, conflicts of interest, entrenched interests, incompetence, and outright corruption are a few of the factors that are turning the issue of voting modernization into a national scandal.

At a time when budgets are constrained everywhere, billions of dollars have been allocated to improve the voting system. Already, hundreds of millions have been squandered on technology that should never have seen the light of day.

One of the ideas for a sweeping solution to the voting problem involves using Direct Record Electronic voting machines, also known as "DREs." The voter makes their selections on a computer screen--often a touchscreen--and then selects a button that says, "Cast my ballot." But where is the ballot? It's invisible! How does it work? "You don't need to know," say proponents. "Trust us," they say.

To the election administrators, DREs seem to solve every problem. They're expensive. But they accomplish everything. They eliminate the need to print paper ballots; they can accommodate voters with special needs; they can easily handle multiple languages; they can tabulate the vote very fast. If they seem too good to be true, it's because *they are* too good to be true. They are absolutely untrustworthy! *The concept of invisible ballots created with secret software is fundamentally flawed.*

Regarding DREs, the consensus opinion of computer scientists and engineers has been well known for a long time. The Association for Computing Machinery, the oldest and largest group focused on computer issues, currently has a poll that is running 95% against DREs. Back in 2000 and 2001, almost every computer scientist asked about paperless DRE voting machines said it's a bad idea. But were they organized to stop them? No, they weren't. Why should they have to organize to stop people from buying these machines? Wasn't it obvious?

Now the computer scientists and engineers are organized against DREs, thanks to David Dill and many others. The days are numbered for the voting machines with the invisible ballots and secret software. In California, as of 2006, paperless DREs will no longer be permitted in public elections. We expect this trend to be nationwide, and we are looking to have a better solution ready to go in the not-too-distant future.

My organization, the Open Voting Consortium, is advocating public software for public elections, and we're building this software now. You may not see OVC software in use in 2004, but you are likely to see it in some jurisdictions in 2005 or 2006. You will see a system with all the advantages of the DREs, except that the voter will print out their finished ballot on the spot. The software will be free and open for public inspection and testing. Companies and governments who use Open Voting Consortium software will utilize off-the-shelf PCs and printers along with our free software so it will be very

inexpensive. No need to warehouse expensive dedicated components! No secrets! A visible ballot!

I am very impressed with the decision-makers here in Utah. You have not jumped into buying voting technology that just isn't ready. I have noticed the thoughtfulness here. Your government is one of the first to join the Government Open Code Collaborative. I believe there are now eight states that have joined, and Utah is one of them. This organization of state and local governments, in collaboration with academic institutions, intends to facilitate the development and use of open source software in governments. This is a great idea and I commend your CIO Val Oveson and his staff for taking this step.

Last Friday, the Utah State Government issued a Request for Proposal, or "RFP," to consider purchasing a VOTING SYSTEM SOLUTION FOR THE STATE OF UTAH ELECTIONS OFFICE. Given the fluidity in the voting technology world, this was a great challenge. It's going to be a difficult process. Your officials took into consideration a great many variables. And yet, this RFP raises many questions.

Utah has taken the extraordinary step of centralizing the purchase decision. This move has its advantages, but it also adds gravity to the decision. Most states allow their counties to make their own voting system purchasing decisions. Your Director of Elections, Amy Naccarato, Val Oveson, and others involved in evaluating responses to the RFP have their work cut out for them. Since computerized voting systems will be included in the bids, I recommend at a minimum that they consult with computer science faculty from leading Utah research universities before drawing any conclusions.

These decisions are coming under closer scrutiny. Every day, we see more articles about what's being done to modernize the voting system--including mistakes that have been made along the way. There is likely to be more coverage on television. Don't try to hide anything! There is no excuse for hiding any part of the public process of voting, including the software code. And, whatever you do, ***don't hide the ballots!***

THANK YOU

Alan Dechert has been a software test engineer and application developer for the past 15 years. In 2001, Alan co-authored a voting modernization proposal for California designed as an in-depth study of the voting system, including development of reference open source voting software. In 2003, along with Dr. Douglas W. Jones (Univ of Iowa) and Dr. Arthur Keller (UC Santa Cruz), he founded the Open Voting Consortium (OVC). He currently serves as President and CEO of the OVC.

Paper v. Electronic Voting Records – An Assessment

[1]
Michael Ian Shamos
School of Computer Science
Carnegie Mellon University
April 2004
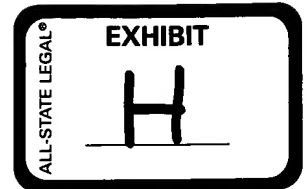
Abstract

There has been much discussion in the popular press concerning the use of contemporaneous paper trails to plug various perceived security risks in electronic voting. This paper examines whether the proposed paper solutions in fact provide any greater security than properly maintained electronic records. We conclude that DRE machines pose a number of security risks but that paper records do not address them. A number of alternatives to paper trails are suggested to respond to DRE security concerns.

1. Introduction

Among the arguments that have been advanced against the use of direct-recording electronic (DRE) voting systems are the following:

1. Voting machines are "black boxes" whose workings are opaque to the public and whose feedback to the voter is generated by the black boxes themselves. Therefore, whether or not they are operating properly cannot be independently verified and the machines should not be used.

2. No amount of code auditing can ever detect malicious or even innocently erroneous software. Therefore the machines should not be used.

3. No feasible test plan can ever exercise every possible combination of inputs to the machine or exercise every one of its logic paths. Therefore the machines should not be used.

4. Hackers can break into the FBI's servers and deface its website. It ought to be child's play for them to throw an election. Therefore the machines should not be used.

5. DRE machines have been plagued by a host of failures all around the country. Therefore the machines should not be used.

6. The DRE industry is dominated by a small number of companies, some of whose executives are announced supporters of the Republican party. An executive could command his programmers to add code to each machine manufactured by that company to move votes to a favored candidate, thus determining the outcome of the election. Therefore the machines should not be used.

7. Many prominent computer scientists have said that DRE machines cannot be trusted. Therefore they should not be used.

[2]

8. If added to a DRE machine, a voter-verified paper trail allows the voter to satisfy herself that her voting preferences have been recognized correctly by the machine. Therefore, the voter-verified paper trail solves every one of the aforementioned problems and every DRE machine should be required to have one.

Each of these arguments will be examined in this paper and found fatally flawed, at least to the extent that it implies that machines cannot be relied upon to count votes in real elections. The numbered statements above all share the property that the first sentence of their premise is true, yet their consequent, that DRE machines should not be used, does not follow from the premise.

In 1993, I prepared a paper for the Computers, Freedom and Privacy '93 conference exploring
[3]
the risks of electronic voting . Since then, I have often been asked whether I still adhere to the

opinions expressed in that paper in light of the incidence of widespread hacking, Internet worms and viruses, new cryptographic attacks and the increased used of DRE machines around the world. The answer is that I still hold those opinions but feel compelled to update the justification for them to respond to the arguments raised above.

Since the Industrial Revolution, man has chosen to rely on machines for tasks that are either impossible for humans to perform, or so expensive or repetitively boring that there is no justification for continuing to waste human labor on them. Many of these machines, such as cars, airplanes and therapeutic radiation equipment, among numerous others, have the capacity to take human life. They also commonly contain embedded computer systems. In the business world we rely on computers to execute financial transactions totaling at least $2 trillion per day. It is well-known that all of these systems present risks. There are approximately 40,000 deaths annually in the U.S. due to automobiles [4] ; some number of the victims are killed by malfunctioning software rather than human error. People have also been killed by the computer programs that control radiation machines [5] . In light of such failures, why do we continue to drive cars, fly on planes and receive radiation treatments? Why hasn't the government outlawed these killing machines?

The reason is that testing and safety procedures are in place that reduce the risks to levels that are deemed acceptable. There is no basis for applying different reasoning to voting machines. Once we decide what a tolerable risk in such systems might be, we can require that the equipment meet that standard. Perfection is never required, expected or even possible in any real system, though it is a laudable aspiration, and perfection is not required, expected or possible in voting systems, either. Federal Election Commission Standard 3.2.1 allows a maximum error rate of 1 in 500,000 voting positions [6] . With a typical ballot size of 235 positions, this is an allowed error of almost one in every 2000 ballots, or 0.2% of the vote.

When the safety procedures are found to have flaws, the flaws are ultimately corrected because of public pressure, government mandate or the relentless law of the marketplace. We are now seeing immense public pressure being put on voting machine manufacturers, along with threats to legislate, both of which are appropriate.

A secondary reason that machines presenting some risk of injury are not outlawed is that people generally have the option not to use a particular machine. This choice is also available to a voter, who may eschew voting machines completely and cast a paper absentee ballot.

While the United States has been using direct-recording electronic voting equipment for well over 20 years without a single verified incident of successful tampering, within the last year a number of people knowledgeable about computer security have questioned whether certain DRE systems in current use are sufficiently secure to be employed safely in elections. Some criticism of these systems resulted from examination of their source code, perceived flaws in their handling and use or from consideration of purely hypothetical scenarios. A calm observer might take solace in the observation that if DREs are so dangerous, then surely at least one security hole would have manifested itself by this time. Realistically, however, hacking has been advancing at a alarming rate, and new attacks are constantly being discovered, so we are entitled only to a small bit of comfort from DRE history.

It is an error, though, to ascribe to DREs generally the bad attributes exhibited by some of them. The spectrum of available systems is broad. Some machines are excellent, some are terrible.

1.1. The "Black Box" Phenomenon

That a machine contains a computer and the computer contains object code not readily viewable or understandable by the public is by itself no reason not to use the machine. If it were, no one ought to own a personal computer. Neither passenger nor pilot can see or understand the software that operates the control surfaces of a jet plane. Such software could contain code, malicious or otherwise, that might send the plane into a dive at noon on a specific date from which the pilot could not recover. How do we

know for a fact that such code is not present? We don't. Yet pilots and passengers continue to board planes every day. Let's look carefully at the reasons we allow jets to operate. All of them apply to voting systems as well.

1. It is beneficial to aircraft manufacturers to make safe planes. Planes that crash will not sell and will eventually be outlawed, not to speak of the legal liability associated with such incidents. This benefit induces the manufacturer to develop internal procedures designed, but not guaranteed, to produce safe products. It is beneficial to voting system vendors to make safe systems also. Whether they know how to do so, or have successfully implemented procedures for doing so, is somewhat questionable. In examining more than 100 different voting systems for certification purposes, I recommended that over 50% of them be denied certification. The quality and reliability of particular DREs is certainly a matter of concern, and later in this paper various solutions will be suggested.

I have heard it expressed that it might not be beneficial under certain circumstances for a voting system manufacturer to produce an honest machine, but that substantial gain could be achieved by distributing machines or software altered to cause the election of specific persons who may not actually be favored by the electorate. We will discuss below the practical difficulties with such a scheme, but if a manufacturer felt that its underhanded activities would not be discovered, such a fraud might be

[7]

attempted despite the possibility of severe criminal penalties   . Therefore any plan for the administration and use of voting machines should contain safeguards against this type of manipulation.

2. Planes are built to high performance and engineering standards. Agreed. Voting machines, which are far simpler than airplanes, can be (but are not always) built to even higher performance and security standards.

3. Planes can be tested. So can voting machines. Neither needs to operate perfectly. Planes shouldn't crash much and neither should voting machines.

4. If a plane crashes, we'll know about it. The significance of this statement, made by DRE opponents, is that we would then at least be able to take remedial action to prevent a recurrence, a fact of little consolation to the victims' relatives. The argument is made that election can be stolen under our very noses and no one would be any the wiser. But that ignores the real political fact that elections are local and local party operatives have an extremely accurate sense of how the community is going to vote. The smell of irregularity is sufficient to set off alarms resulting in investigations and recounts. DRE opponents claim erroneously that in a disputed election there is nothing useful left to recount since all the records that remain were made by the malfunctioning machine. But this argument is wrong because the software that was used in the machine survives. (We can deal later with the assertion that the software might modify or delete itself to evade discovery.)

5. The people who fly airplanes have a vested interest in their safety. The people who run voting systems are likewise committed to clean elections. Pilots have been known to crash planes deliberately and election officials have been known to manipulate votes. Safeguards need to be built in to prevent both of these efforts from succeeding.

In short, I am unable to discern any engineering difference that allows us to entrust our lives to aircraft but would impel us to avoid voting machines. Not to endorse questionable voting systems or trivialize the possibility of chicanery, but I believe I and the republic will survive if a president is elected who was not entitled to the office, but I will not survive if a software error causes my plane to go down.

1.2. Computer Security

It is pointless to discuss the security of a computer system in the absence of a well-articulated list of threats. So let's enumerate and deal with them in order.

1. Isolated attacks on individual machines. There are any number of ways of interfering with the operation of any computer system, such as pounding on it with a sledge hammer or the slightly more sophisticated technique of exposing it to several watts of radio-frequency emission. Such efforts fall into the class of mischief rather than tampering because they cannot be used to cause a predetermined result.

A different form of attack is to gain access the hardware or software of an individual machine or small number of such machines and alter them, either by connecting to ports and interfaces or by opening the machine by force or with the help of an insider who may have the keys, along with manuals, plans and source code listings for the machine. It should be obvious that no machines should be used that allows any voter to connect to it electrically to during an election and any device that permits this should be decertified immediately. The question is how to prevent people from modifying the machines offline or at least to be sure the tampering will be detected before the machines are used.

One solution is to ensure that all software needed to operate the machines, including the operating system, is not installed in the machine until election day. The authorized, certified software, distributed from a central authority (not the manufacturer), can be brought up at the time the polls are opened. In this way no advance modification of any software would be fruitful. If it is deemed undesirable to do a full machine boot, a portion of the code can be loaded on election day and verify through message digests and encrypted checksums that none of the prestored files has been altered.

2. Attacks by hackers or insiders at a polling place. The tendency to use networked voting machines at polling places for ease of administration also increases the risk that an insider could use a computer connected to the network to distribute malware to the voting machines after the election has begun. The miscreant would presumably remove the malicious code or restore the original at some time before the end of voting so that no trace would remain of the misdeed. This sort of attack presupposes that the insider is able to erase evidence of his deed during the election, for if the altered software is still present in the machine at the close of polls it can be detected. It also is a highly localized manipulation that affects the results at a single precinct only.

3. Attacks by hackers or insiders at a central count facility. Now the magnitude of the problem grows because the number of votes that are potentially affected can be extremely large. There are 35 counties (out of a total of 3170) in the United States with populations exceeding 1 million [8]. The total population of these counties is over 73 million, approximately 25% of the country's population. A successful attack on central count systems in these 35 counties, (representing just 1.1% of the total number) would certainly influence any election, so every step must be taken to prevent such an event. Fortunately, in most states the results produced at central count stations are informational only, and are not the official election returns. With DRE systems, the ballot images representing individual voters' choices are stored both in the machine on which they were cast in redundant memories and also in removable modules than can be transported. All of these memories are cryptographically linked so substitutions and cracking are not feasible. A manipulation of the central count computer would not be to any avail since the totals produced there would not correspond to the canvass of individual precincts.

4. Insertion of malicious code by the machine manufacturer. There are two subcases. In the first, the manufacturer delivers software to a jurisdiction with prior knowledge of the ballot layout, candidate names, etc. for each precinct in the jurisdiction. The machine is programmed to behave perfectly before and after the election but to switch votes to favored candidates during the election. This manipulation is possible if the manufacturer is able to distribute software directly to specific precincts prior to an election. Countermeasures are discussed in sections 3.5 and 3.6, below.

In the second subcase, the manufacturer has no foreknowledge of the details of any specific election but distributes master software that causes candidates of a particular party to win in all future elections. The practical possibility of such a scheme is nil. There are about 170,000 election precincts in the United States. It is not possible to move a constant fraction of votes from one party to another in each jurisdiction without it being obvious that manipulation is going on because the political demographics of the precincts are too individualistic and distinctive. Therefore the software would have to be distributed with a database telling it how to alter the vote for each relevant candidate in each precinct. The database would have to contain at least the names of political parties and possibly candidates and would have to know in advance the precise hours during which all future elections are to be conducted so the machine would know when to behave properly.

This nightmare scenario, in which a small number of programmers manipulate the politics of the

United States by injecting undetectable malicious software into voting machines has more in common with spy novels than it does with reality. For example, in the movie *Goldfinger* (1964), a crazed collector of gold apparently uses nerve gas to kill the entire garrison of troops guarding Fort Knox, then enters the vault where U.S. gold is stored and almost sets off an atomic device that would render the U.S. bullion supply radioactive and useless, which would immensely increase the value of his own holdings. When the film appeared, did the Army close Fort Knox out of fear that the plot was realistic? No. The reason is that adults eventually develop the ability to distinguish fact from fiction, a critical intellectual facility that should not be abandoned simply because we are talking about voting. Did the Pentagon evaluate the plot to determine whether there were security weaknesses that ought to be remedied? Probably. Were some security procedures modified to reduce the probability that such a plot would succeed? Maybe. Is breaking into Fort Knox in such a manner absolutely impossible? No. Why, then, if there is some nonzero probability that a person could do it, do we allow our gold to remain stored there? It's because we never require perfection in real systems. We balance the risks rationally against the cost and other detriments of preventing the risks and make a reasoned determination. Just because a novelist (or a computer scientist) can dream up an entertaining doomsday plot involving voting machines does not mean we should toss them on the junk heap.

The argument I have with DRE opponents is that they insist that any conceivable risk of any kind of manipulation is unacceptable. That standard is never applied anywhere in human affairs, and there is no reason it should apply to voting, despite appeals to patriotism and pious claims that our very constitutional system is in jeopardy.

I do not propose that machines or software ought to be trusted just because they use advanced technology. In his 1984 Turing award lecture, entitled "Reflections on Trusting Trust," Ken Thompson demonstrated a method of hiding malware so it absolutely cannot be detected by any amount of

[9]

examination of the corresponding C source code   . The technique involves corrupting the C compiler so that it recognizes certain patterns in the source program and compiles them into object code that performs not as written but as the malicious intruder intends. Of course if one is able to modify the compiler in this fashion the compiler could just substitute an entire program of its own choosing upon reading a "signal" string in the source text. Efforts to test the compiler to reveal its misbehavior would be frustrated unless one knew the signal string, since if the string were missing the compiler would always perform properly. Theoretically this hack enables arbitrary amounts of code to be inserted into any program at the cost of introducing but a short sentinel string to tell the compiler to start its dirty business.

[10]

The Thompson Trojan horse is frequently cited by opponents of electronic voting   as a reason not to rely on voting machines. No one has ever suggested a remotely practical manner in which the world's compilers could become corrupted, but let's assume there is some way of sneaking a rogue compiler into a huge number of computers. This ignores the fact that jurisdictions themselves do not compile voting software, and that even though the source code may not be revealing, the object code contains all the evidence necessary to detect the intrusion. A decompiler can be used to verify that the malware is not present and/or that the object code being used corresponds to the original object code.

The argument has even been made that Turing's proof of the undecidability of the Halting

[11]

Problem has some applicability to DRE machines   . The cited paper asks us to draw the conclusion that "Determining that software is free of bugs and security vulnerabilities is generally impossible." That statement is true only if the word "generally" is carefully defined. A correct version of the statement, but one unsuited to the opponents' purposes, is "There is no procedure that is always *guaranteed* to determine whether an arbitrary program is free of bugs and security vulnerabilities." The unsolvability of the halting problem does not imply that no program can be proven correct, nor does it imply that the halting problem for restricted programs is unsolvable. For example, FOR-loops that do not modify the index variable or its limits and contain only straight-line code do halt. These are

precisely the type of loops that are used for iteration in vote tabulation.

Assuming that one believes it is necessary for voting system vendors to produce mathematical proofs that their software is correct (an unreasonable proposition), one can easily imagine structuring a program that reads a finite number of ballot images and produces vote totals to be amenable to such a proof. I therefore must brand references to undecidability in the context of electronic voting simply as sophistry.

1.2.1. The Omniscient Hacker

Combining the misleading Halting Problem argument with the Ken Thompson code-hiding method produces a fantasy that I refer to as the "omniscient hacker," which was explained to me by an opponent of DRE machines who will probably be grateful not to be named here. The hypothetical omniscient hacker is able to insert arbitrary amounts of malware into a voting system in such a way that it can never be detected by any amount of code reading (source or object) or testing (before, during or after the election), yet is able to alter the votes to achieve any predetermined result in any jurisdiction for an arbitrary numbers of years into the future. We need not yet go into the details of why such a thing is or is not possible, since a moment's reflection reveals such a hypothesis to be no more than a purely religious belief. By the very premise of the statement the malware cannot be detected, so no amount of evidence of its non-existence can disprove the statement. If the malware ever is detected, the hacker will explain that he just didn't do a good enough job hiding it, but he'll succeed the next time. In this way belief in the omniscient hacker is indistinguishable from belief in a Supreme Being. There is simply no argument one can give that will dissuade a true believer, yet when the believer is asked for a demonstration he is unable to produce one.

That said, here is an adversary argument that demonstrates that the omniscient hacker cannot exist, though for the reason just stated I do not expect true believers to accept it. If we test the machine during the election by feeding it votes in a manner indistinguishable from regular voting, the malware must decide whether it is going to tell the truth or lie about the vote count. If it tells the truth, it has disabled itself and we need not be concerned that it is present. If it decides to lie, we will catch it, since we are casting a set of ballots whose totals are known.

It is of course possible that there are ballot combinations we may not have tried that will cause the malware to enter lying mode, but there is little risk that ordinary voters will happen upon those combinations either and the malware is either effectively silenced or it will be caught. One can imagine a magic input to the machine that will cause to begin lying (such as writing in the name "Turing" for President). But then activating this feature on every voting machine, or even a substantial number of them, would require a conspiracy of huge proportions.

By its very definition there can be no defense against the omniscient hacker, since we would never be able to tell whether he has been thwarted. (We might as well postulate the existence of an omniscient tamperer who is able to substitute an arbitrary number of voter-verified paper trails without detection. There's no defense against him, either.) Belief in omniscience is a matter of faith. Those who really accept the possibility of an omniscient hacker will never be satisfied with DREs.

1.3. Voting Machine Standards

Since 1990, the Federal Election Commission has developed and promulgated Voting System
        [12]
Standards   . The current version of these standards is now several hundred pages long. They deal with hardware, software, telecommunications, security, qualification, testing and configuration management, among other issues. They are voluntary in that any state may, but is not required to, adopt the standards as part of its voting system certification process. As of this date, 36 states and the District of Columbia have done so. The standards are clearly a step in the right direction and obviously enjoy widespread state support, although one wonders whether the states have really evaluated the standards and found them to be meritorious or have adopted them for convenience. It is difficult, however, for a standards-making body to keep up with developments in computer security, develop countermeasures

for newly-recognized threats and document them in the form of precise standards. Thus Volume I Standard 6.4.2, entitled "Protection Against Malicious Software" is just two sentences long: "Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status." An Independent Testing Authority (ITA) would be justified in claiming that the standard gives no operational guidance in testing a system to see whether it is secure against malicious code. It also appears to pass the burden to vendors, who are the very parties against whom we seek protection.

[13]

Independently of the FEC Standards, Section 301 of HAVA   purports to impose certain

[14]

minimum standards on "each voting system used in an election for Federal Office."   The term "Federal Office" is not defined in the statute but the Department of Justice takes the position that it has the meaning defined for it in other Federal election statutes, namely, "the office of President or Vice President, or of Senator or Representative in, or Delegate or Resident Commissioner to, the Congress." Laying aside for a moment the question whether Federal control of Federal elections is a good or bad thing, Section 301 of HAVA is unconstitutional on its face. While the Congress may make rules

[15]

concerning elections for senators and representatives   , it has no power to specify standards for presidential elections. Article II, Sec. 1 of the U.S. Constitution reads in part: "Each State shall appoint, in such Manner as the Legislature thereof may direct, a Number of Electors, equal to the whole Number of Senators and Representatives to which the State may be entitled in the Congress ... The Congress may determine the Time of chusing the Electors, and the Day on which they shall give their Votes; which Day shall be the same throughout the United States." Thus Congress has no power to determine the manner in which presidential electors are chosen other than to specify the time and date of their election.

No one seems to have noticed this unconstitutionality, but more probably the states simply do not care, since HAVA allocates billions of dollars to them for acquisition of voting machines – a case of not acknowledging that the gift horse even has a mouth. In any case, HAVA does not deal at all with the problem of malicious software.

1.4. Testing

DRE opponents argue that DRE software may contain up to 50,000 lines of poorly-written code

[16]

that is impossible to read or test   . The argument is misleading – deliberately so in the author's opinion. It is true that complete voting software systems, including ballot setup and printing components, may reach that size, but the portions of code that accept input from the voter and record ballot images – the very portions suspicions about which have given rise to calls for paper trails – are tiny by comparison.

While it is surely true that not every logic path of a computer program of any size can be exercised, this is obviously not a reason not to use software. Otherwise no commercial software would ever be used, and surely not in any situation in which human life were at risk. The issue is whether any combination of code reading, program testing, open source code publication and other techniques can give us adequate assurance that the software does not contain malicious code or logic errors that will cause votes to be altered. The answer is certainly yes. If code is too obscure, or contains portions that are not readily understandable, it should not be used. Only if the relevant programming is transparent and available to the public should we be confident about using it.

One should realize that the basic loop that interrogates portions of a touchscreen and interprets them as votes is not very complex, although an entire election administration system might be. When the user touches the screen the processor is notified through an interrupt and receives the geographic coordinates of the point that has been touched. A search is made to determine which box on the screen

has been touched. Any code that is present that treats candidates differently based on their ballot positions should not be there.

1.5. Machine Failure

By far the most justifiable criticism of DRE machines is that they fail during service or in some cases cannot even be brought into service on election day. There are numerous documented instances of such failures. These incidents are real. They are intolerable when they interfere with the act of voting.

It is important, however, to understand the nature of the machines' failure modes. They do not suddenly decide to move votes from Democrats to Republicans. They may "hang up," refusing to accept any more votes. The mechanical components, particularly the touchscreens, may develop dead spots or fail to register at all. Switches and buttons wear out. Circuits exhibit erratic behavior. These situations can result in severe voter inconvenience and loss of confidence in the process. Long lines can develop, causing voters to balk and go home. The sight of technicians opening machines and replacing components in full view of the voters does not promote trust in the integrity of elections.

While voter inconvenience is certainly detrimental, the critical question is whether any votes are actually lost or modified when the machines fail. In properly designed DRE, no vote once cast is ever lost because ballot images are stored in redundant memories, including write-once devices. It is possible, however, for a machine to fail in such a way that votes cast subsequent to the failure are misrecorded. When the failure is discovered later, it may be too late to reconstruct the lost votes. This situation is akin to mechanical failure of a lever machine – regrettable, but not fatal so long as the failure is not systematic or deliberately induced.

The matter of machine reliability is a question of design, engineering, testing and adherence to maintenance procedures. The responsibility of the vendor is not to be overlooked. A proper voting machine procurement will impose heavy penalties on vendors whose machines do not conform to warranty. If a jurisdiction is unwilling to rely on indemnification by a vendor, a solution is to acquire spare machines and stand ready to deploy them as needed during an election.

It is the author's opinion that many of the so-called failures of DREs in fact resulted from inadequate training of poll workers in using the equipment. HAVA has created an incentive for counties to rush to procure and begin using DREs. Some jurisdictions have done so without adequate preparation, and have seen failures occur during an election. When machines are tested at the warehouse immediately prior to an election and are found to be working, yet cannot be started on election day morning, it is much more likely that the problem results from unfamiliarity with startup procedures than a sudden and unexplained failure of the equipment.

Despite energetic efforts by opponents to slow their adoption, DRE machines continue to be adopted at a prodigious rate. India, the world's largest democracy with over 650 million voters recently adopted DRE machines nationwide. Just its 600,000 villages constitute more than four times as many election districts as there are in the entire United States.

2. Paper Trails

It has been asserted that adding paper trails to DREs allows prompt detection of all of the possible intrusions discussed above. It is based on the mistaken belief that paper records are in some way more secure or free from tampering than electronic ones, which is not the case.

On March 20, 2004, a presidential election was held in Taiwan. The winner by 29,518 votes (out of over 13 million cast) was the incumbent, Chen Shui-bian. To achieve this result, the Central Election Commission had to declare 337,297 ballots as invalid, more than 11 times the supposed margin of victory. The voting method was by paper ballot, and there weren't even any DRE machines to blame. Surely if the voters could rely on the paper ballots to be counted properly this result could not have occurred.

2.1. Paper Records

Humans have a profound affinity for that which they can see and touch. This results in a deep reverence for the printed word, whether it is true or false, and explains the comfort people derive from paper receipts. There are very few paper documents that have preclusive legal effect, meaning that the writing on the face of the document is not subject to challenge.

There are basically four types of paper records:

1. Bearer instruments. Examples: currency, bearer bonds, checks, movie tickets. Here the instrument itself entitles the bearer to rights with no further inquiry into his bona fides. Title to the document passes with possession. These instruments are extremely convenient for transactions because they can convey rights and title instantaneously without resort to offline records and databases. They are also a frequent subject of theft.

2. Receipts. Instead of being a instrument used to effectuate a transaction, a receipt is merely evidence of the transaction. As such, a receipt takes its place among all of the other forms of evidence, including spoken words, videotapes, witness testimony, business records, computer databases, etc. The receipt confers no independent rights, but is given for several reasons. First, a party to the transaction usually insists on a receipt (a) as evidence of the transaction, as in an ATM withdrawal; (b) to verify the correctness of its details, as in a restaurant bill; (c) as an aide-memoire to recall the transaction. It is used in the event of a dispute to lend credence to the claim of one party or another. The contents of a receipt may be challenged or rebutted and the effect it has will be determined by the trier of fact.

3. Business records. These are notes kept by a business as part of its operations. Records kept in the ordinary course of business are admissible as evidence, but they are only evidence and may be challenged. They differ from receipts in that they are created by one party to a transaction and but are not normally reviewed for correctness by the other party. A dispute between a bank and its customer over a questioned ATM transaction usually turns on the question of which records are more credible, the customer's paper receipt or the bank's computerized business records.

4. Ballots. A ballot is an expression by a person indicating how she wishes to cast her vote. A ballot is a unique document defined by election law and is itself only evidence of how a voter wanted to vote. A ballot may be challenged on many grounds, including an allegation that the voter was not entitled to vote, the ballot was mismarked, the voter voted in the wrong precinct, the voter cast votes for candidates she was not entitled to vote for, the ballot was mangled, defaced or was otherwise unreadable. In many, but not all, states when the content of a ballot is disputed, a court is required to determine the intent of the voter in marking the ballot and is not bound by that the ballot actually says.

There are numerous other forms of paper records, such as documents of title, licenses, wills, diplomas, written offers, etc., that are not relevant to our discussion here. The question is what desirable properties, if any, do paper records have that would cause us to prefer them over electronic ones for voting.

The largest industry in the world in terms of daily cash flow is foreign currency trading, which often totals more than $2 trillion per day. The entire world securities industry rarely exceeds one-tenth of that amount, and no sector that deals in physical goods can even approach it. The vast majority of foreign currency trades are made without any use of paper whatsoever, either in the form of an original order or a generated receipt. If computers are unsafe and hackers and well-placed insiders lurk behind every door, one wonders why the traders don't lose a billion dollars a day (or at least a million) as a result of malware. In December 2003, no less a figure than Senator Hilary Clinton stated while

[17]

introducing her "Protecting American Democracy Act of 2003 ": "You go to an ATM, you get a receipt. You play the lottery, you get a ticket. Yet when you cast your vote, you get nothing. The systems used by the people of the United States to exercise their constitutional right to vote should be as reliable as the machines people depend on to get their money. What's required for money machines should be required for voting machines." Statements that play well to the electorate often fail when subjected to the cool light of logic.

[18]

Sen. Clinton is correct that Regulation E of the Federal Reserve Board requires a financial

institution to make a receipt available when a consumer initiates an electronic funds transfer at an ATM. She might be surprised to learn how limited the legal effect of the receipt turns out to be. If a financial institution fails to provide a receipt through "inadvertent error," it is not in violation of Regulation E [19]

. Furthermore, the receipt itself is only prima facie proof (subject to rebuttal) that the consumer [20]

made a payment to a third party   . It is not proof of the amount of transfer and is of course of no effect at all in the case of an ATM deposit, since the data associated with the deposit is generated completely by the consumer, not the bank.

In the event of a later dispute between the consumer and the bank, the ATM receipt is evidence only and is not dispositive of the question what amount was transferred. The bank may challenge the data on the receipt based on its own records. Note that the receipt has been in the hands of the consumer and thus has been subject to alteration or forgery, which means that the document itself cannot be given absolute effect. Of course in electronic banking transactions initiated over the Internet there are no paper receipts at all, yet this fact has not dampened enthusiasm for online banking.

The law governing ordinary sales transactions, the Uniform Commercial Code, gives no legal [21]

effect to receipts and certainly does not require them   . In fact, neither party to a sale transaction has the legal right to demand a receipt, although it may be a customary business practice to comply with such a demand.

Sen. Clinton would be positively dismayed to learn that a lottery ticket has even less value to its holder than an ATM receipt. State lottery rules typically provide that if a dispute arises between the holder of a lottery ticket and the state lottery bureau, the computer records of the lottery bureau govern. This New Hampshire Lottery rule is illustrative: "To be a valid ticket and eligible to receive a prize … [t]he information appearing on the ticket shall correspond precisely with the Commission's computer [22]

record."   The lottery rules clearly provide that computer records govern over paper ones.

And so it must be. If presentation of a small piece of paper were sufficient to claim a prize of [23]

$363 million   , the inducement to fraud and bribery to produce a counterfeit ticket would be extreme, and the nature of paper is that it would be essentially impossible to invalidate the ticket based on a physical examination because genuine ticket stock can easily be obtained. This raises the question what the purpose of a lottery ticket might be if not to ensure the buyer that he will get paid in the event of a win. Despite what the public might believe, the lottery ticket is simply a receipt, that is, an item of evidence that can be considered in the event of a dispute. It also provides the buyer with the opportunity, in the act of buying a ticket, to verify that the human operator typed in his numbers correctly. The issue is not that the lottery ticket machine may have malfunctioned, but that the human seller may have made a mistake. (As we have seen, if the lottery machine malfunctions, that is, communicates a different set of numbers to the lottery commission than those printed on the ticket, the buyer has no effective recourse.) Because the only human in the voting booth is the voter herself, and the voter has ample opportunity to review her ballot, the verification function of the lottery ticket is not relevant to elections.

The lottery ticket also serves to remind the buyer which numbers he chose so he can later compare his numbers with the winning ones. It is also necessary to claim the prize, since a lottery ticket is anonymous and transferable. The state must know whom to pay. None of these considerations is [24]

applicable to voting   .

Of course Sen. Clinton's Protecting American Democracy Act of 2003 is unconstitutional for exactly the same reason that Section 301 of HAVA is unconstitutional – it purports to allow Congress to legislate standards for presidential voting, a privilege reserved to the states.

When I raise the point to opponents of electronic voting that huge volumes of commerce are

conducted based only on computer records, their answer is, "If anyone lost a billion dollars they would know. If someone steals votes, we'll never know." This explanation is appealing, but specious. If someone were able to manipulate a bank's computer records to spirit away a huge sum of money, it is reasonable to believe that he could do so while at the same time not only deleting any computer records of the transaction but also modifying the bank's records so it did *not* know there was any loss. But in any event it does not matter whether the bank knows that it has lost a billion dollars or not – the money is gone and the risk the bank tried to avert has occurred anyway.

2.2. Electronic records

The areas of human endeavor in which electronic records are used in place of paper ones are far too numerous to list. Among them are banking transactions, income tax filings, medical diagnosis, military orders (including nuclear launch instructions) and securities purchases.

The public and the legal system have come to recognize that electronic records can be reliable if properly maintained. The Electronic Signatures in Global and National Electronic Commerce Act ("E-Sign")[25] raises electronic records to at least equal dignity with paper ones. It provides that in "any transaction in or affecting interstate or foreign commerce … a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form."[26] There are a small number of exceptions for such specialized documents as wills and testamentary trusts and notices of termination of insurance benefits, but otherwise electronic records do not have inferior status.

The regulations implementing the E-Sign statute generally provide that electronic records are equivalent to those on paper[27]. The Uniform Electronic Transactions Act (UETA) has been adopted in 45 states and is pending the three others. UETA specifies the legal effect of electronic records and has as one of its stated purposes "to promote public confidence in the validity, integrity and reliability of electronic commerce and governmental transactions."[28] If electronic records are questionable in some way, how has this fact escaped the vast majority of our state and federal legislators?

The Federal Rules of Evidence give equal weight to electronic records in court proceedings as they do to paper ones[29]. It is therefore a puzzle why electronic records should be acceptable for every other government purpose except voting. Neither E-Sign, UETA nor the Federal Rules of Evidence contain any receipt requirement.

2.3. Paper ballots

Paper ballots can be divided generally into those that are intended to be read and counted by humans, which we shall call Australian ballots to avoid ambiguity, and those intended to be counted by machine. The latter included punched-card and mark-sense (optical scan) ballots.

Every form of paper ballot that has ever been devised can and has been manipulated, in general with considerable ease. The reason is that humans are familiar with paper and its characteristics, how to mark it to look genuine and how to erase it. Likewise, the number of people in the U.S. capable of producing professional printed matter is huge. There are over 50,000 printing companies in the U.S, employing over 1.2 million people, of whom more than 100,000 are prepress operators[30]. This means that it is not difficult to locate people who can print or modify documents.

Other types of manipulation, such as destroying ballots or substituting other ones, require no skill at all. By contrast, altering redundant encrypted write-once computer records is impossible even for experts. So assuming that the electronic voting records are written correctly in the first place (a subject that indeed deserves discussion), the possibility of modifying them later is remote.

The simplest form of paper ballot manipulation is ballot-box stuffing, that is, inserting extra ballots, usually genuine ones that have been pre-marked, into the container meant to hold only those voted by registered voters. In any jurisdiction in which the voter can touch a physical ballot and personally insert it into a ballot box, she can conceal extra ballots on her person and insert them at the same time. This is true whether the ballots are Australian, punched-card or mark-sense. The practice is so widespread that many states have statutes specifically dealing with the situation in which more ballots are found in the ballot box at the close of voting than the number of voters who appeared at the polls that day. The Florida statute is both horrifying and amusing: "[I] if the number of ballots exceeds the number of persons who voted, as may appear by the poll list kept by the clerk and by the stubs detached by the inspectors, the ballots shall be placed back into the box, and one of the inspectors shall publicly draw out and destroy unopened as many ballots as are equal to such excess."   [31]   Yes, ballots are chosen at random and discarded until the totals come out right! The most appalling thing about the law is not how the procedure is to be conducted, but that the situation occurs frequently enough that the law had to be drafted in the first place.

Actually, the Florida process solves nothing except to avoid the unseemliness of having more votes cast than voters, which is always an embarrassment. If the ballot box has been stuffed, the random discard process will not alter the candidates' percentages on average. That is, whoever wins by the stuffed vote total will probably also win after the excess votes are tossed away, and the stuffers will have achieved their objective.

Another form of manipulation is to perform substitution of ballots on a large scale. In central-count jurisdictions, ballots are not counted at polling places but are transported by vehicle to a centralized counting station, usually at the county seat. The ballots are carried in transport cases outfitted with locks and seals, but the locks can easily be opened and the seals counterfeited. It can take several hours in large counties for the ballots to reach the counting station, giving ample opportunity for chicanery. Instances are known in which manipulators did not even bother to open and reseal the ballot cases, but merely substituted others that had been prepared once the total turnout in each precinct became known. This sort of manipulation is made easy by the fact that printed Australian ballots are insecure and transport cases and seals easily obtained from unauthorized sources.

One of the oldest and easiest forms of tampering is to invalidate an Australian ballot while touching it. When I was in middle school during the 1950s, our American history teacher explained that poll workers would break off a piece of pencil lead and insert it under their thumbnail. When they found a ballot voted for a candidate they didn't like, they would make a second mark for some other candidate in the same office, thus creating an overvote that had the effect of erasing the undesirable choice. Once this has been done, there is no effective way to reconstruct the original ballot.

Because Australian ballots have to be marked and read by hand, there is no real prospect for tampering to occur on a national scale. The same is not true of punched-card and mark-sense ballots. The only remaining use of punched cards in the United States is for voting, and only two manufacturers remain in the business. Without giving a catalog of possible tampering methods, there are many parameters in card manufacture than can be varied to the advantage of one candidate or another if the voting positions corresponding to the candidates are known at the time of manufacture.

The problem of hanging chads, long known in the election industry, came to public attention in Florida in 2000. But for years many states used "chad teams," groups of poll workers who function was to tear loose chads from ballots before they were fed into the card reader. Once we allow a person to alter a ballot that has been cast by a voter, anything is possible. A perfect tool for punching out chads by hand is the metal tongue from an ordinary waistbelt. Small and easily concealed in the hand, it can be used the same way the old pencil lead was employed to overvote Australian ballots.

With mark-sense ballots it is known that if the areas for marking the ballots are printed improperly or the timing marks at the side of the ballot are skewed, votes that are cast will not be read properly by the scanning machine. More tampering is possible through the selective application of inks that appear white but absorb the infrared light that is used in the reading process. An answer, one might

think, is that we always have the original ballots around to recount by hand, but mark-sense ballots are just as susceptible to loss, substitution or augmentation as Australian ones.

In general, the rampant problems with paper ballots are neither acknowledged nor addressed by opponents of electronic voting, who seem oblivious to the fact that their opposition to new technology, if successful, will compel us to retain something that is much worse.

2.4. The "Voter-Verified" Paper Trail

It is alleged that adding a so-called "voter-verified paper trail" to a DRE machine will either permit tampering to be detected or at the very least will provide a reliable record of how each voter voted that can be used for a recount, even if the recount must be conducted by hand. This is incorrect. A paper trail accomplishes one thing, and one thing only – it provides assurance to the voter that her vote was initially captured correctly by the machine. This is no small accomplishment, but it can be achieved in numerous other ways, as explained below. That is the only voter-verified part. The paper trail provides no assurance at all that her vote will ever be counted or will be counted correctly. The reason simply is that the paper trail itself becomes insecure at the moment of its creation.

First, if the machine cannot be trusted, which is the working hypothesis of paper trail proponents, then it cannot be trusted to deal with the paper trail safely. After the voter leaves the voting booth, it can mark her ballot as void and print a different one. The voter will have left the booth believing not only that her vote was cast and counted properly, but that it will also be counted properly in any recount. None of these beliefs is correct.

One might argue that inspection and testing of the machine would reveal such abjectly bad behavior, but the claim of DRE opponents is that no amount of inspection and testing is ever sufficient. If testing is adequate to reveal paper trail flaws, then it is adequate to uncover other faults in the machines.

Here is a further, but only partial, catalog of problems with paper trails.

1. The paper trail cannot be on a continuous roll of paper, since that would permit reconstruction of each voter's ballot based on the order in which votes were cast. Therefore, the paper trail must consist of separate pieces of paper. However, once the pieces of paper are separated, the integrity of the trail is lost. Looking at a piece of paper, we will not be able to tell for certain where it came from. Stuffing and all other paper ballot tampering methods then become possible. The addition of cryptographic indicia, which has been proposed as a method to prevent insertion of unauthorized ballots, cannot work since the voter will never know whether her real ballot contained the proper indicia when it was created. If it didn't, the ballot will not be tabulated during a recount.

2. Adding a paper printing device to a DRE machine naturally adds another component that can fail, run out of ink, jam or run out of paper. If DREs are alleged already to be prone to failure, adding a paper trail cannot improve that record. In Brazil in 2003, where a small number of precincts had installed paper trails, failure of the printers delayed voters by as much as 12 hours, a figure that would be
[32]
catastrophic in the U.S.

3. There is no voter-verified paper trail machine that has been tested on any large scale.

4. States that propose to implement the paper trail have promulgated regulations stating that the paper
[33]
shall govern over the electronic record in the event of discrepancy   . This has the effect of making the insecure paper record paramount over the secure electronic one, a return to the early days of the Australian ballot.

5. With complex ballots, voters are prone to forget exactly whom they have voted for. When confronted with a paper record, they may erroneously claim that the machine made a mistake. This will call the machine's reliability into question, prompt calls for a recount and cast doubt even on machines that are functioning properly.

6. Paper trails do not address the problem of DRE failures. If the complaint is that a machine cannot be initialized for use on the morning of election day, then having a paper trail mechanism is of no help. In

fact, the presence of the mechanism increases the load on the machine's power supply and processor and itself increases the probability of failure.

7. The paper trail requires a re-examination of meaning of the terms "ballot" and "official ballot." This is not a mere semantic exercise, but a question of great legal and, in some states, constitutional significance. Can a piece of paper be a ballot if it is neither marked nor touched by the voter? If so, significant statutory changes will be required. If the paper is the ballot, then what conceivable meaning can be ascribed to the computer count, which is not derived by counting the "ballots," but by processing the voters' original inputs that were separately used to generate the ballots? If the paper ballots are official, then we are put in the untenable position of having to certify an election without ever actually counting the ballots, unless an allegation of irregularity compels a "recount."

8. Each losing candidate will claim that the election was stolen from him by the machine and will insist that the only true indication of the voters' preferences reside on the paper, even if there is no evidence of irregularity or tampering. Thus paper recount will become the default method of vote counting, mitigated only by the high cost of such recounts. If this is to be the case, why use voting machines in the first place?

9. Paper trails cannot readily be viewed by disabled voters, requiring them yet again to reveal their votes to strangers in order to have them verified. It is no answer to say that there are other mechanisms to review their votes. If paper trail proponents truly believe the paper trail is necessary for fair elections, then elections will not be fair for the disabled.

10. A report of the Caltech-MIT Voting project concluded that the presence of paper trails actually decreases public confidence in the voting system [34]. This can be understood as follows: would requiring airplane passengers to inspect the plane's engines before boarding enhance their belief in the safety of the aircraft?

My position on paper trails, despite their problems, is not an extreme one. If a manufacturer produced a reliable paper trail device and the remainder of his system were acceptable, I would see no problem in certifying such a machine. I am firmly opposed to any audit trail requirement, however, and even where audit trails are used, the paper record should never govern over the electronic one because it is vastly less secure. The proper use of audit trails is as evidence. If the paper trail totals differ from the electronic ones, that is the starting point for investigation, not the end of the issue..

3. Alternatives to Paper Trails

If paper trails are not the answer, are there practical alternatives that will not only render DREs safe but also persuade the public that they are safe? Let us assume that all of the security risks discussed above (except the omniscient hacker) are realistic. Are there measures other than paper trails that will prevent them? The author does not discount the importance of assuring the voter that the machine is working and that her preferences have been collected without error. This can be done in a multitude of ways that do not involve paper.

3.1. Audit devices

A prime motivation for audit trails is the possibility that the machine has been programmed improperly, either by accident or by design, or that rogue software has been substituted for the authorized version. Suppose we were to require voting machines to be architecturally separated into two distinct devices: a panel, possibly but not necessarily a touchscreen, whose only function is to display the ballot and capture voter choices, and a tabulation and recording device, which accepts input from the panel and performs computations. The panels and tabulation devices could be supplied by different manufacturers.

Now suppose we feed the output of the panel to two different devices simultaneously. One is the tabulation machine; the other is an audit device made by yet a third manufacturer and programming by an independent body, such as an accounting firm or public interest group not affiliated with the tabulation manufacturer. The audit device displays the voter's choices on a screen of its own for

verification. The voter views the audit screen, and if it is correct, presses a "VOTE" button. Both the tabulation device and the audit device make redundant read-only records of each ballot image. At the end of the election, all the records are compared. If they different in any respect whatsoever, the results from that machine are called into question and an investigation is launched. An examination of the software installed in the two devices should reveal whose records are the reliable ones.

So long as there is no collusion between the audit device manufacturer and the tabulation manufacturer, no amount of tampering with either machine will go unremedied. The prospect of tampering identically with both, since their software systems would be completely different, is too small to consider seriously. The audit device could easily be outfitted so disabled voters could verify their votes.

3.2. Open source

The manufacturers of voting equipment claim that their software is a trade secret and go to extraordinary lengths to preserve that myth. The author has been looking at the source codes of voting systems for over 20 years and has yet to find any significant differences in their design except possibly for the number of bugs they contain. They all do the same thing, albeit in somewhat different ways. No vendor's software is a significant selling point providing any competitive advantage over other systems – jurisdictions focus on the hardware. All the software has facilities for setting up elections, storing the candidate and party names in a database, presenting ballot choices to the voter, tabulating and storing the results and possibly transmitting them after the election. The systems vary in ease of use and capacity, but they do not contain trade secrets for the simple reason that every aspect of election setup and balloting is well-known to all.

One might speculate then on why they try to keep the source code confidential. The uncharitable view, which appears to have some justification, is that they don't want the public to see how bad their code is. A legitimate reason might be to avoid making matters easy for competitors, but that does not justify withholding information from the public that is necessary to promote confidence in the electoral process. Another reason is to hide security measures which, if disclosed, would provide a roadmap for hackers. I am somewhat sympathetic to that view, despite the meaningless but mocking phrase "security through obscurity," since I know a thief will have a much harder time stealing my car if he does not know where I have hidden the key than if he does, and a party who happens to find my hidden key will have no idea which car it fits.

On the other hand, there is no reason that the ballot setup, display, tabulation and reporting sections of voting system code should be kept secret, and manufacturers would be wise to accede to public demand in this regard.

3.3. Administrative procedures

The administrative procedures concerning the handling of DRE machines and materials are usually not spelled out at all, or, if spelled out, then not circulated and not followed. Many of the observed vulnerabilities in DRE systems stem not from problems of machine design, but from lax handling procedures. A thorough election administration manual should explain at least the following steps:
1. Custodianship of machines at all times, including transportation to and from polling places.
2. Receipt and registry of software to ensure that only authorized copies of everything, including operating system versions, are used in voting machines.
3. There should be no delivery of any software directly from vendors to jurisdictions; otherwise (2) will not be observed.
4. Deposit and security for ballot materials, including any election programming. Likewise, control of installation of election programming into voting machines.
5. Chain of custody for any removable media containing ballot images or vote totals.
6. In the event an audit trail is used, chain of custody for the paper ballot images.
7. Freezing of machines and their software at least until the election is certified and the time for any

challenge has passed.

8. Exception procedures for handling irregularities during an election, including custody of partial totals on any machine that is removed from service.

3.4. Standards

It may not be fruitful to have all the states separately ponder and solve the myriad of problems in election administration posed by the sudden introduction of new voting technology. Knowledge and experience should be pooled and election officials ought to be able to rely on a full set of standards, including security and vote handling procedures, that they can follow. The FEC Standards were principally written for ITAs to follow, not for election jurisdictions, and do not specify processes that are responsive to numerous objections that have been raised to DRE voting.

The budget provided by HAVA is fully sufficient to fund development of a comprehensive set of standards and procedures which, if followed, would greatly diminish the number of problems observed at polling places.

3.5. Parallel testing

More than 15 years ago, in a Pennsylvania certification report, I wrote of the possibility that a DRE machine could contain an on-board clock and that an intruder could rig the machine so that it behaved perfectly in all pre- and post-election tests, but switched votes during an election. The prospect is even more real today than it was then, since computers now routinely possess such clocks. This attack presupposes that the software knows all dates and times for elections into the indefinite future, but let's assume it has such knowledge [35] .

One solution is to forbid on-board clocks altogether, but that would limit various other capabilities, such as making a time-stamped record of happenings during the election. It also raises the question how one can tell whether a clock is present in a machine or not. The second obvious solution is to reset the machine's clock to a time on election day, run a test and then set the clock back to the correct time. This is ineffective since the machine could contain software that would detect such a change and know that it was being watched.

A better solution is to employ parallel testing, a plan originally suggested by this author that was used in 10 counties in California during the 2004 primaries. Under this method, a set of examiners is empowered to enter any polling place at the start of voting and commandeer any voting machine for test purposes. No actual voters cast votes on the selected machine. No change whatsoever is made to the test machine – it is not even moved from its position (to counter the argument that it might contain a motion sensor to warn that it was under test). The examiner votes a number of predetermined ballots comparable to the number that would be voted on a typical machine in that precinct. Of course, manual entry of votes by a human is an error-prone process, so a video camera is used to capture his actual vote entries. At the normal close of polls, the votes on the test machine are tabulated and compared with the expected totals. If any software is present that is switching or losing votes, it will be exposed.

The function of this test is limited. It of course does not ensure that even one other machine in the precinct is working properly. It is designed to detect the nightmare scenario in which some agent has tampered with every machine in the jurisdiction undetectably, a major risk cited by DRE opponents to justify the addition of paper trails.

The examiners would select precincts and machines at random on the morning of the election. It is an issue of statistical quality control exactly how many precincts should be chosen. This testing, while cumbersome, is much easier that statutorily mandated recounts in which a certain percentage of ballot images must be totaled manually.

3.6. Separation of candidate names

Perhaps the ultimate protection against malicious code is to keep candidate and party names segregated from the software so it cannot perform any meaningful manipulation. If the machine is

programmed to move votes from one party to another, it will be stymied if it is unable to determine the party with which a candidate is affiliated or even which candidate is associated with a given ballot position. This can be done by presenting the candidate and party names and issue text in the form of graphic files that can only be read by a human being. The only thing the software can do us faithfully record the numbers of the ballot positions that were selected. Of course, since it also knows no candidate names, it can only report results by ballot position. To defeat such a countermeasure the software would have to contain a complete optical character recognition algorithm.

It is possible that in a conspiracy a tamperer's confederate could, while voting, provide information via touchscreen selections or the write-in panel that could inform the software of the particular voting positions to manipulate. However such an act would have local effect only, since it would take one confederate for each voting machine involved. It would not be feasible to perform manipulation on a large scale with such a scheme.

4. Answering the Objections

We are now equipped to respond to the objections to DRE voting raised in the Introduction.

Objection 1. DREs are black boxes. So are all other computer systems, on which we rely for our lives and our fortunes.

Objection 2. Code cannot be audited. Yes, it can. Not all code can be audited, and we can bar unauditable code from being used in elections. We can also make the code available for scrutiny by an arbitrarily large audience by making source code open.

Objection 3. Machines cannot be tested. Why not? Every other type of machine can be tested, and voting machines are not nearly as complicated as airplanes.

Objection 4. Hackers can do anything. Only in books and movies. The hacking stories we read in the papers concern attacks over the Internet against systems that are deliberately held open for access by the general public. Voting machines, by contrast, are highly controlled and cannot be accessed over the Internet. Hackers are not omniscient and even vendors have trouble programming tabulation software correctly. The prospect that a hacker could not only manipulate an election but do it without exhibiting a detectable bug is so far-fetched an idea that no one has come close to showing how it might
[36]
be done   .

Objection 5. DREs are failing all over the place. The answer here is simple: buy reliable ones. The FEC Standards specify numerous tests designed to weed out unreliable hardware.

Objection 6. The vendor can rig the machines. But we can expose him through any number of mechanisms, including audit devices and parallel testing. An we can render his manipulations fruitless by separating candidate and party names from the capture and recording logic.

Objection 7. Computer scientists say DREs are unsafe. Since when was this technological issue to be decided by popular vote rather than by analysis? There are over one million computer scientists
[37]
and mathematicians in the United States   . About 100 of them have signed a resolution in favor of
[38]
paper trails proposed by www.verifiedvoting.org   . No information is available on how many have any familiarity with the processes of voting or the actual architecture of DRE machines, but the total number represents about 1 in 10,000, a minuscule proportion. The good news seems to be that the other 9,999 out of 10,000 have remained open-minded on the subject.

Objection 8. Paper trails meet objections 1-7 and make DREs minimally acceptable. As we have seen, this is not true. The paper trail does no more than persuade the voter that her vote was initially captured properly, but at the risk of announcing to the voter that the whole process is so insecure that her own vigilance is necessary. If the voter has to be watching at the polling place, what sort of confidence will she have in the remaining procedures that are conducted outside her presence? We have shown a number of alternatives to paper trails that genuinely meet the objections raised.

[39]

DRE machines have been described, somewhat dramatically, as a threat to democracy   . A far greater threat to democracy is a return to any form of paper ballot, but both of these pale in comparison to the fact, not widely known, that in each presidential election more than 5 million Americans who are eligible to vote and want to vote are unable to cast a ballot because they happen to be outside their home districts on election day and cannot comply with their state's absentee procedures. Many of these people are overseas. The claim that tens of thousands of Floridians were disenfranchised in the 2000 election because of butterfly ballots, though probably true, is insignificant when measured against the millions who were unable to obtain any ballot at all. If computer scientists are truly concerned about threats to democracy, that's one they should work on.

---

[1]

The author is Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University and an attorney admitted to practice in the Commonwealth of Pennsylvania and before the United States Patent and Trademark Office. From 1980-2000 he was statutory examiner of electronic voting systems for the Commonwealth of Pennsylvania. From 1987-2000 he was the designee of the Attorney General of Texas for voting system certification. During those years he personally examined more than 100 different computerized voting systems for certification purposes. In the 2000 election, machines for which he participated in certification (which did not include Florida) were used to count more than 11% of the popular vote of the United States. This paper was prepared to accompany the author's appearance on an electronic voting panel at the ACM Computers, Freedom & Privacy Conference held in Berkeley, California in April 2004.

[2]

The feminine pronoun is used to drive home the fact that a majority of U.S. voters are women.

[3]

Shamos, Michael, "Computerized Voting – Evaluating the Threat." Proc. Third ACM Conf. on Computers, Freedom & Privacy. San Francisco, CA (Mar. 1993). Available at http://www.cpsr.org/conferences/cfp93/shamos.html.

[4]

National Transportation Safety Board Publication NTSB/SR-02/02, "Safety Report: Transportation Safety Databases," September 11, 2002. Available at http://www.ntsb.gov.

[5]

Leveson, Nancy et al., "An Investigation of the Therac-25 Accidents," *IEEE Computer 26,* 7, pp. 18-41 (July 1993).

[6]

Available from the Federal Election Commission website at http://www.fec.gov/pages/vssfinal/vss.html.

[7]

N.Mex. Stat. Ann. 1-20-5 provides, "Unlawful opening of a voting machine consists of, without lawful authority, opening, unlocking, inspecting, tampering, resetting or adjusting a voting machine owned by any county, or conspiring with others to have the same done. Whoever commits unlawful opening of a voting machine is guilty of a fourth degree felony." In general, tampering is a felony but the penalties are probably not sufficiently high. *Quaere* whether under the New Mexico statute a manufacturer who ships rigged software would in fact be committing this crime, which seems to require modification of a machine after is has become owned by a county.

[8]

U.S. Bureau of the Census, "Population Estimates for the 100 Largest U.S. Counties: April 1, 2000 to July 1, 2002," available at http://eire.census.gov/popest/data/counties/tables/CO-EST2002/CO-EST2002-09.php. Six of the 35 counties are in New York; another six are in California.

[9]

Thompson, Ken, "Reflections on Trusting Trust," *CACM 27,* 8 pp. 761-763, August 1984.

[10]

Neumann, Peter, "Risks in Computerized Elections," Inside Risks 5, *CACM 33,* 11, p.170, November 1990

[11]

Jefferson, David et al., "A Security Analysis of the Secure Electronic Voting and Registration System (SERVE)," Jan. 21, 2004. Available at http://www.servesecurityreport.org/paper.pdf.

[12]

Available from the Federal Election Commission website at http://www.fec.gov/pages/vssfinal/vss.html.

[13]

There is one reference in HAVA to the FEC Standards, but it pertains to acceptable error rates in ballot counting. 42

U.S.C. §15481(a)(5).
[14]
     42 U.S.C. §15481(a).
[15]
     Article I, Sec. 4 of the U.S. Constitution provides: "The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators."
[16]
     Bannet, John, "Hack-a-Vote: Security Issues with Electronic Voting Systems," *IEEE Security and Privacy Magazine*, Jan/Feb 2004.
[17]
     Bill S. 1986, 108th Congress, First Session.
[18]
     12 C.F.R. §205.9.
[19]
     12 C.F.R. §205.17.
[20]
     12 C.F.R. §205.17.
[21]
     There is a type of document of title known as a "warehouse receipt," which is necessary for a buyer to secure possession of his goods in certain situations, that has special status under the Uniform Commercial Code. But this is not the sort of receipt one ordinarily receives from a merchant in a sale transaction.
[22]
     New Hampshire Lottery Rule 7(C).
[23]
     The largest U.S. lottery payout in history, $363 million, resulted from the May 9, 2000 drawing in The Big Game, a multistate lottery now known as "Mega Millions."
[24]
     In his CFP '93 paper the author endorsed the use of state lottery systems for voting (without giving receipts, of course) and still does because their security and reliability is proven daily all around the country and they are clearly trusted by the public.
[25]
     15 U.S.C. §7001 ff.
[26]
     15 U.S.C. §7001(a)(1).
[27]
     The Food and Drug Administration regulations are typical: "Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper." 21 C.F.R. §11.1(c).
[28]
     UETA Comment 1(f).
[29]
     F.R.E. 1001 reads, "For purposes of this article the following definitions are applicable: (1) Writings and recordings. 'Writings' and 'recordings' consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation."
[30]
     Press release of the Indiana Business Modernization and Technology Corporation, Dec. 21, 2001.
[31]
     Fla. Stat. §102.061.
[32]
     Mira, Leslie, "For Brazil Voters, Machines Rule," *Wired News*, Jan. 24, 2004.
[33]
     Standard 2.1.1.4, "State of California DRAFT STANDARDS For Use of Accessible Voter Verified Paper Audit Trail Systems in Direct Recording Electronic (DRE) Voting Machines," Secretary of State of California, March 18, 2004.

[34]
    Selker, Ted. et al, "The SAVE System: Secure Architecture for Voting Electronically: Existing Technology, with Built-in Redundancy, Enables Reliability," CalTech/MIT Voting Project VTR Working Paper, Oct. 22, 2003, revised January 4, 2004.
[35]
    It is actually not difficult to deduce this information from the ballot programming, which usually contains the date of the election in a predefined text field, the presence of which could be required by the system.
[36]
    See note 16. Hack-a-Vote is a project in which students are asked to develop malicious vote-counting software and other students try to find the malicious portions. It's not easy when posed in that framework.
[37]
    According to the Bureau of Labor Statistics, in 1990 there were about 881,000 computer scientists and mathematicians in the U.S.
[38]
    Spannaus, Edward, "Electronic Voting is Threat to the Constitution," *Executive Intelligence Review*, Jan. 30, 2004.
[39]
    Zetter, Kim, "How E-Voting Threatens Democracy." Wired.com, Jan, 29, 2004.
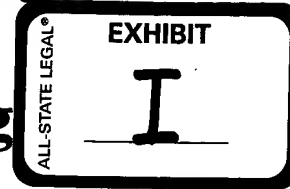
OVC Response to Paper v. Electronic Voting Records -- An Assessment, by Michael Ian Shamos

This message: [Message body] [More options]
Related messages: [Next message] [Previous message]

From: Alan Dechert <*alan_at_openvotingconsortium_dot_org*>
Date: Fri Jul 30 2004 - 22:11:03 CDT

Michael Ian Shamos is often quoted by individuals and organizations that want to say DREs are the way to go. He is a highly credible individual, so what he says on this subject matters a great deal.

The more I look at it, the more his arguments seem incredibly bad. David Jefferson, a friend of Shamos for 30 years, has said that he is doing a lot of damage and his POV on DREs should be discredited.

Here is a paper he wrote for the CFP 2004 conference we were at.

http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm#_edn1

I have made a rough first cut at a response. I'd like to go through a few iterations on this and then distribute it to the press and other interested parties.

****
OVC Response to Paper v. Electronic Voting Records -- An Assessment, by Michael Ian Shamos

Professor Shamos published this paper in April of 2004. This paper is deeply flawed, but it deserves a careful response for three main reasons:

1) The OVC is flatly opposed to invisible ballots (DREs) created with secret software. Shamos argues in favor of invisible ballots.

2) Professor Shamos in one of few prominent scientists that argues in favor of invisible ballots. His testimony is often used by organizations seeking to bolster their support of DREs.

3) Although some of his arguments appear to be wrong, Professor Shamos makes many excellent points worthy of consideration and support.

Shamos shows a fondness for defeating arguments no one is making. The paper is full of strawmen. It appears that Shamos has not really followed or considered what some of the leading thinkers in this area have been saying. He mischaracterizes or ignores them.

The title itself is weak. "Paper v. Electronic Voting Records" is not really the issue here. We want to know where the authentic vote exists. Should it be purely electronic? He does not consider the possibility of paper ballots (where the actual vote exists) produced with computerized voting systems where there is also an electronic audit trail. He does not discuss ideas for reconciling paper and electronic records.

He starts by listing eight claims made by DRE opponents. Then he says, "Each of these arguments will be examined in this paper and found fatally flawed.." Could it be that he constructed these 8 arguments in such a way that they could be easily refuted?

> 1) Voting machines are "black boxes" whose workings
>   are opaque to the public and whose feedback to the
>   voter is generated by the black boxes themselves.
>   Therefore, whether or not they are operating properly
>   cannot be independently verified and the machines
>   should not be used.

The issue here is not so much about whether they can be independently verified: it's that they aren't independently verified [to be operating properly]. Certainly, they cannot be verified with black box testing alone.

> 2) No amount of code auditing can ever detect malicious
>   or even innocently erroneous software. Therefore the
>   machines should not be used.

Again, this is not really the issue. It's not about whether the auditor can spot malicious or erroneous code during a code audit, it's about whether or not they will. Given the track record of code that has been certified, it appears auditors have a very limited focus in these code audits.

> 3) No feasible test plan can ever exercise every possible
>   combination of inputs to the machine or exercise every
>   one of its logic paths. Therefore the machines should
>   not be used.

I suppose that every professional test engineer knows that the first sentence is absolutely true [for software of medium or better complexity]. This fact by itself is not why paperless voting systems should not be used, but it's part of the reason.

> 4) Hackers can break into the FBI's servers and deface its website.
>   It ought to be child's play for them to throw an election.
>   Therefore the machines should not be used.

Who is making this argument? Generally, it's true that hackers come up with remarkable tricks that no one thought possible.

> 5) DRE machines have been plagued by a host of failures all

around the country. Therefore the machines should not be used.

These failures illustrate some of the costs/benefits of DREs. Right now, it appears that many jurisdictions have spent a lot of money on technology that is immature and that will be obsolete soon. It just looks like a bad investment.

> 6) The DRE industry is dominated by a small number of companies, some of whose executives are announced supporters of the Republican party. An executive could command his programmers to add code to each machine manufactured by that company to move votes to a favored candidate, thus determining the outcome of the election. Therefore the machines should not be used.

While some have characterized paperless voting as a Republican conspiracy, this is small minority of critics. Interestingly, we are seeing some Republicans saying that Democrats will use paperless systems to rig the vote. The OVC position is that it must be assumed that all people involved in election administration, as well as all the voters, are partisan. The integrity of the voting system must not depend, at any point, on people (or groups of people) being honest, non-partisan, or uninterested in the outcome. The integrity of the voting system can only be assured with a system of checks and cross-checks.

> 7) Many prominent computer scientists have said that DRE machines cannot be trusted. Therefore they should not be used.

It's not so much that so many have said that. It's what they say about it.

> 8) If added to a DRE machine, a voter-verified paper trail allows the voter to satisfy herself that her voting preferences have been recognized correctly by the machine. Therefore, the voter-verified paper trail solves every one of the aforementioned problems and every DRE machine should be required to have one.

No one is making this argument. This is a pure strawman.

Shamos rambles on saying, "Since the Industrial Revolution, man has chosen to rely on machines for tasks.." This part has some interesting points, but none of it has anything to do with paperless voting. We all know that technologies bring various risks as well as advantages. Shamos completely misses the point.

The point with DREs is the possibility of rigged elections with no possibility of recovering how voters actually voted. We are suspicious of malicious insiders, and for good reason. If conspirators are given a way to throw an election, we must assume they will try since we know it has been

done in the past. Cheaters are everywhere.

If there is a large enough conspiracy, no amount of careful voting system
design can prevent it. However, we can make a conspiracy unlikely by
requiring such a large amount of cooperation that it is bound to fail. The
weakest voting system would be one where a single conspirator could throw an
election. Paperless voting introduces the possibility that a single person
with the requisite knowledge and access could throw an election. We can
also imagine scenarios with a few insiders with a few outside confederates
that could change the outcome of an election.

Shamos argues that we can make aircraft software reliable, so we can trust
software for voting machines without the need for a paper audit trail. His
analogy does not hold. The threat model is not similar. Safety in aircraft
software is a goal common to all involved. Everyone wants it to be safe to
fly. Shamos mentions that planes have been deliberately crashed but this is
extremely rare.

We find substantial agreement in Section 3.2 regarding open source. Shamos
concludes, "On the other hand, there is no reason that the ballot setup,
display, tabulation and reporting sections of voting system code should be
kept secret, and manufacturers would be wise to accede to public demand in
this regard."

Section 3.3 has some good suggestions for handling DREs, but doesn't this
also show some of the hidden costs of DREs? More time, expertise, manpower,
etc. are needed to ensure the integrity of these machines.

I fully agree with Section 3.4. Probably, Shamos was not talking about the
OVC as coordinator of this federally funded effort to develop standards.
But I think we are developing a very strong group of scientists and
engineers that could do this work.

In section 3.5, Shamos talks about some parallel testing that was employed
with DREs. He admits that it has limited value. But it's worse than that.
This type of testing is very expensive since it requires another DRE for
each pollsite, and can only find certain types of problems that are unlikely
to occur. He says, "It is designed to detect the nightmare scenario in which
some agent has tampered with every machine in the jurisdiction undetectably,
a major risk cited by DRE opponents to justify the addition of paper
trails." It really has almost no value the way it is described because it
wouldn't even detect what he says it is designed to detect. That is, it's
possible that every machine has been tampered with while parallel testing
would not detect it because the tester does not know the trigger for putting
the machine in rigged mode.

Shamos is at his absolute worst when he says, in effect, to the people that
say these machines could be rigged (or have been rigged), "show me." He
wants people to show him how this has been done or could be done. It
apparently means something to him if no one shows him.

Why would anyone be willing to show him? Consider the case of slot machine rigger, Ronald Harris. Suppose you were defending the slot machines for their lack of bias. Would it be particularly meaningful to issue a challenge to see if anyone could hack one of these machines? Before he was caught, would Ronald Harris have been interested in meeting your challenge? Even if you offered a reward of $10,000 or more, why would Harris be interested in revealing his scheme when he could reap hundreds of thousands or even millions by keeping his secret? In fact, Harris was a slot machine examiner that figured out a way to insert code such that the machine would payout the jackpot if you inserted coins in a certain pattern. If you know the combination ("signal string"), you get the jackpot: Otherwise, it behaves just like every other slot machine (Harris was only caught because his confederate acted very suspiciously after winning a $100,000 jackpot, and Harris was found in the confederate's hotel room).

Now consider the stakes involved in just local elections. Billion dollar projects have been won or lost with a single vote in the City Council. Local officials are often involved in decisions that involve many millions of dollars. If someone has figured out a scheme for rigging voting machines, they will not be interested in telling you about it for the same reason Harris would not have been interested in telling you about his slot machine rigging scheme. If they have successfully tested the scheme in an election, they would be guilty of a felony and probably will not want to admit that. Furthermore, if they took such a risk, they probably are expecting some large future rewards. They may be hoping to make millions by throwing a single local election. They won't be interested in telling anyone about it in advance (other than co-conspirators).

After strenuously arguing that it couldn't be done, Shamos seems to admit that it could be done. But he dismisses the threat because it would only be local.

"It is possible that in a conspiracy a tamperer's confederate could, while voting, provide information via touchscreen selections or the write-in panel that could inform the software of the particular voting positions to manipulate. However such an act would have local effect only, since it would take one confederate for each voting machine involved. It would not be feasible to perform manipulation on a large scale with such a scheme."

Is Shamos trying to say that unless you can overcome a several percent difference nationwide in a presidential contest that it's not important? I don't think we can dismiss "local effects." As previously mentioned, local contests (City Council, County Supervisor, ballot measures, etc) can carry very large financial impacts. And local effects could even decide a national contest in a Florida 2000 situation where a few hundred votes swung one way or the other could make the difference. The voting system is as bad as its weakest link. Even if a particular type of manipulation cannot be done on a large scale, it is unacceptable to permit it.

4. Answering the Objections

Shamos goes over each of the eight objections he identified at the outset
and attempts to summarize how he has defeated these objections. Some of
these summaries are truly incredible. For objection no. 7 (computer
scientists say DREs are bad), he uses his estimate that "About 100 of them
have signed a resolution in favor of paper trails proposed by
www.verifiedvoting.org" to conclude that "the other 9,999 out of 10,000 have
remained open-minded on the subject." His math here is positively shameful.
The ACM poll is currently running 95% against DREs (in favor of voter
verified paper trails). The list of independent (i.e., those not on the
payroll of DRE makers) computer scientists speaking out in favor of DREs
seems to begin and end with Shamos.

Finally, Shamos cites voter disenfranchisement due to poor absentee ballot
systems. He says, "If computer scientists are truly concerned about threats
to democracy, that's one they should work on." He has mischaracterized this
as an either/or option. This is not a choice we have to make. This is
just another big problem-one of many-with the voting system. If we want to
have a great voting system instead of the bad one that we have now, there is
a lot of work to do. It's a very big job.

Alan D.

Received on Sat Jul 31 23:17:15 2004

This message: [Message body]
Next message: Jan Karrman: "New PDF file"
Previous message: Barbara Simons: "Re: FW: Has the (Ohio) ACLU gone over to the Dark
Side?"

Contemporary messages sorted: [By Date] [By Thread] [By Subject] [By Author] [By
messages with attachments]

This archive was generated by hypermail 2.1.8 : Sat Jul 31 2004 - 23:17:15 CDT

ⅢⅰⱤЄⅡ ᴺᴱᵂˢ

Home | Technology | Culture | Business | Politics | Wired Mag | Animation
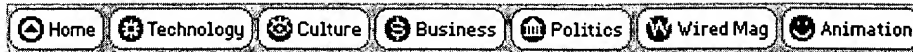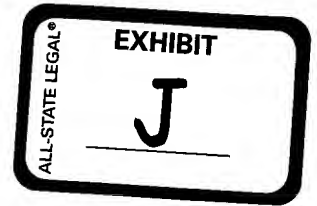
Text Size: A A A A

California Bans E-Vote Machines

By Kim Zetter | Also by this reporter

03:53 PM Apr. 30, 2004 PT

California Secretary of State Kevin Shelley ended five months of speculation and announced Friday that he was decertifying all electronic touch-screen voting machines in the state due to security concerns and lack of voter confidence.

He also said that he was passing along evidence to the state's attorney general to bring criminal and civil charges against voting-machine-maker Diebold Election Systems for fraud.

"We will not tolerate deceitful tactics as engaged in by Diebold and we must send a clear and compelling message to the rest of the industry: Don't try to pull a fast one on the voters of California because there will be consequences if you do," he said.

Shelley said the ban on touch-screen machines would stay in effect unless and until specific security measures could be put in place to safeguard the November vote.

"Revelations regarding touch-screen machines have shaken public confidence in this voting technology," Shelley said, referring to four computer-science reports released in the last year that showed the machines to be badly designed and vulnerable to hacking. "It is my foremost responsibility to take all steps necessary to make sure every vote cast in California will be accurately counted."

At least four counties will not be able to use touch-screen machines at all in November because they purchased a type of Diebold machine that was never federally certified.

But Shelley held out hope for 10 counties that currently own other types of touch-screen machines by saying the state would consider recertifying the machines on a county-by-county basis for November if the counties could meet a long list of stringent security requirements. County officials also must adhere to a number of directives for Election Day. If they don't meet

the requirements, then they will have to use a paper-based voting method, such as optical-scan machines, which use a paper ballot that officials then scan into an electronic reader.

Additionally, Shelley declared that no county or vendor would be able to make last-minute changes to voting systems. Such changes caused problems in at least two counties in the March primary where a malfunctioning Diebold device prevented hundreds of polling places from opening on time.

"That horrific process stops now. We saw what it resulted in on March 2nd," Shelley said.

Finally, all counties will have to provide voters with the option of voting on a provisional paper ballot if they feel uncomfortable casting votes on the paperless e-voting machines. Shelley said that voting companies would bear the brunt of the estimated $1 million cost for providing extra provisional ballots to every county, indicating that the vendors caused the erosion in voter confidence, so they would have to pay for the solution.

"I don't want a voter to not vote on Election Day because the only option before them is a touch-screen voting machine. I want that voter to have the confidence that he or she can vote on paper and have the confidence that their vote was cast as marked," Shelley said.

The state would bear the cost of some of the other changes, such as helping to replace touch-screen machines with optical-scan machines in counties that can't meet the stringent security requirements before November.

Yahoo.com

Wired News: Staff | Contact Us | Advertising | RSS | Blogs | Subscribe
We are translated daily into Spanish, Portuguese, and Japanese

EarthLink®

PRINTER-FRIENDLY FORMAT
SPONSORED BY

FREE HOROSCOPE   choos Taurus
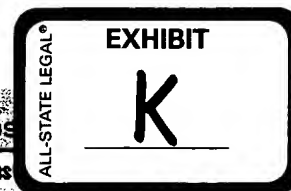
print this page

Prototype E-Vote Printer Fails to Satisfy

February 03, 2005 9:48 PM EST

SAN JOSE, Calif. - Three months after the presidential election, one of the nation's biggest makers of touch-screen voting machines has created a companion printer that spits out paper records.

The prototype that Diebold Inc. is now touting is exactly what some critics of the ATM-like machines have been demanding for several years.

Even so, paper records alone are not enough to satisfy computer scientists who say transparency in the electronic machines' design and software must complement paper backups.

The Diebold prototype seeks to reassure voters by displaying their selections under a piece of glass or plastic alongside the touch-screen machine. If they spot a problem, they can cancel the ballot and start over. And while voters can't touch the paper records, elections officials will be able to use them to verify close elections.

"Results in the last election reflected the accuracy and security of the (paperless) system," said Diebold spokesman David Bear. "But the fact of the matter is, there are some states that are demanding printers."

After months of criticism by computer scientists that electronic voting systems are unreliable, California and Illinois recently passed laws requiring a paper trail for electronic ballots, and at least 20 other states have considered similar legislation.

Critics of North Canton, Ohio-based Diebold say the AccuView Printer Module is a step in the right direction but doesn't address the potential for buggy software or malfunctioning hardware that could misrecord votes or expose voting systems to hackers, deletions or other disasters.

The printers are only valuable to the extent that counties use them, and critics worry that county elections officials with tight budgets may not opt for them.

Computer scientists also are concerned that the handful of private laboratories licensed to certify voting equipment, including the printer module, still operate in secret and without any federal guidelines.

"It's a very, very small step forward in terms of security of elections," said Avi Rubin, technical director of the Information Security Institute of Johns Hopkins University and co-author of a scathing report on Diebold machines.

Like many computer scientists, he thinks paperless voting systems should be banned.

"I'd say a Diebold machine with a paper trail is better than a Diebold machine without a paper trail, but that's as positive I can be about it," Rubin said.

Diebold stock price rose sharply in the months after the presidential election, when the machines fared far better than critics had predicted. But executives warned investors last week not to expect more dramatic improvements from its voting equipment division. The company's stock hit a 52-week high of $57.75 in mid-January, and closed at $54.91 on Thursday.

About 40 million Americans cast electronic ballots during the Nov. 2 election, but only 2,600 touch screens in Nevada - made by Oakland, Calif.-based Sequoia Voting Systems Inc. - and a few other prototypes around the

country produced paper records.

Some of the paperless systems were blamed for high-profile failures in November that included these:

- In Carteret County, N.C., where paperless machines failed to retain 4,438 votes during early voting, one Democratic incumbent lost by 2,287 votes out of about 3 million cast. Courts and the state elections board are deciding how to handle the missing ballots, but the winner of the agriculture commissioner race still hasn't been determined.

- About three dozen voters in six states complained that they tried to select Democrat John Kerry, but the touch screens showed them as having voted for President Bush until they revised their ballot. Equipment manufacturers blamed miscalibration.

- And in a Franklin County, Ohio, a precinct where 638 voters cast ballots in the presidential election, a computer recorded 3,893 extra votes for President Bush. The error was corrected in the certified vote total.

Even with the printer, breakdowns and paper jams are possible, said Stanford University computer scientist David Dill, a leading touch-screen critic.

Others say printers only compound the complexity of the nation's patchwork of voting systems. Counties must pick from hundreds of models of voting equipment, maintenance contracts, software and hardware upgrades, consulting services and other add-ons.

Because no federal agency enforces certification standards, one voter advocacy group is creating a Consumer Reports-style ranking for voting equipment.

The Voting Systems Performance Rating would create standards and assign grades on such factors as reliability, security, privacy and accessibility for the visually impaired. States and counties could use such rankings to help them decide which products to purchase.

"You can't solve the voting problem unless you have a totally transparent mechanism to evaluate," said a founding member, David Chaum, a Los Angeles cryptographer. "In order to crack this voting systems nut, you have to do it in the broad light of day."